Online Safety Policy Template for schools

Scottish Government
Riaghaltas na h-Alba
gov.scot

Contents

Introduction

This portfolio of school Online Safety Policy templates is intended to help leaders produce a suitable Online Safety Policy which will consider all current and relevant issues, in a whole school context, linking with other relevant policies such as a school's child protection / safeguarding, behaviour and anti-bullying policies.

The requirement that learners are able to use digital technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Schools must, through their Online Safety Policy, meet their statutory obligations to ensure that learners are safe and are protected from potential harm, both on and off-site. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

These policy templates suggest policy statements which could be considered as essential in any school Online Safety Policy, based on good practice. In addition, there is a range of alternative statements that schools should consider, given their particular circumstances.

An effective Online Safety Policy must be tailored to the needs of each school and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the whole school community.

It is suggested that consultation in the production of this policy should involve a wide range of interested groups e.g. teaching and support staff; learners; community users and any other relevant groups.

The Scottish Government has set out its vision for digital technology in Education as follows: "Scotland's educators, learners and parents take full advantage of the opportunities offered by technology in order to raise attainment, ambition and opportunities for all". The National Action Plan on Internet Safety for Children and Young People states: "The internet is central to the lives of the majority of children and young people. We want children and young people to be protected, safe and supported in the online world and for them to be able to enjoy the internet, show resilience and take advantage of the opportunities it has to offer"

Due to the ever-changing nature of digital technologies, it is best practice that the school reviews their Online Safety Policy at least annually and, if necessary, more frequently in response to any significant new technological developments, new threats to online safety or incidents that have occurred.

With its optional statements and guidance notes, this portfolio of templates is longer than the resulting policy document is likely to be. It is intended that, while covering this complex and ever-changing issue, the resulting policy document should be concise and easily understood if it is to be effective and adopted by all. The templates are based on current best practice policies and procedures and schools can amend them to suit their own requirements.

Guidance notes

- Within the templates, sections which include information or guidance are shown in BLUE. It is anticipated that schools would amend or remove these sections from their completed policy document, though this will be a decision for the school group that produces the policy.
- It is strongly advised that sections formatted in **BOLD** are retained, as they should form an essential part of a school's Online Safety Policy.
- Where sections in the template are formatted in *ITALICS*, it is anticipated that schools would wish to carefully consider whether to include that section or statement in their completed policy.
- The first part of this document (the first approx. 30 pages) provides a template for an overall Online Safety Policy for the school. The appendices contain acceptable use agreement templates and more detailed, specific policy templates. It will be for schools to decide which of these documents they choose to amend and adopt.

[Name of school]

Online Safety Policy

This policy applies to all members of the school community (including staff, children / young people, volunteers, parents and carers, visitors, partners, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Version: [?}

Date created: [00/00/00]

Next review date: [00/00/00]

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of [*INSERT SCHOOL NAME*] to safeguard members of our school community online in accordance with principles of open government and with the law. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the school community (including staff, children / young people, volunteers, parents and carers, visitors, partners, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

[INSERT SCHOOL NAME] will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Policy development, monitoring and review

This Online Safety Policy has been developed by the *[insert group/committee name e.g. Online Safety Group]* made up of: (delete/add as appropriate)

- *headteacher/senior leaders/Senior Management Team*
- *online safety lead*
- *child protection/safeguarding lead*
- *staff – including teachers/support staff/technical staff*
- *parents and carers*
- *partners*
- *community users*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for development, monitoring and review

This Online Safety Policy was agreed by the school on:	*Insert date*
The implementation of this Online Safety Policy will be monitored by:	*Insert name of individual/group/committee (e.g. online safety lead, senior leadership team, other relevant group)*
Monitoring will take place at regular intervals:	*Insert time period (suggested to be at least once a year)*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Insert date*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Insert names/titles of relevant persons/agencies, e.g. local authority ICT service, local authority Child Protection lead officer, duty social work team, police*

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using: (delete/add as relevant)

- *logs of reported incidents*
- *monitoring logs of internet activity (including sites visited)*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
    - *children/young people*
    - *parents and carers*
    - *staff.*

Policy and leadership

Responsibilities

In order to ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours,

learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Local Authority:

Schools should work very closely in partnership with officers from their authority to ensure that their school policies and procedures are in line with local and national advice and inter-agency approaches to the safety and wellbeing of children and young people.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- The headteacher ensures that staff are aware of online safety risks and their mitigations, while having the confidence to embrace digital technologies.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- *The headteacher/senior leaders will receive monitoring reports from the Online Safety Lead, as appropriate.*

Online Safety Lead

NOTE: It is strongly recommended that each school should have a named member of staff with responsibility for online safety; some schools may choose to combine this with the child protection/safeguarding lead role. Schools may choose to appoint a person with a child wellbeing background, preferably with good knowledge and understanding of the new technologies, rather than a technical member of staff – but this will be the choice of the school.

The online safety lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials

- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

The online safety lead will:

- lead the Online Safety Group
- work closely on a day-to-day basis with the child protection/safeguarding lead, where these roles are not combined
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned and embedded
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/parents/carers/learners
- liaise with (school/local authority) technical staff, pastoral staff and support staff (as relevant)
- report regularly to headteacher/senior leadership team.
- liaises with the local authority/relevant body.

Curriculum leads e.g. Principal Teachers

Curriculum Leads will work with the online safety lead to develop a planned and coordinated online safety education programme. This will be provided (amend/delete as relevant) through:

- *across the curriculum*
- *a discrete programme*
- *personal, social & health education*
- *assemblies and pastoral programmes*
- *through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.*

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they have the skills and knowledge to use digital technologies safely and responsibly
- they understand that online safety is a core part of safeguarding
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to *(insert relevant person)* for investigation/action, in line with the school child protection procedures
- all digital communications with learners and parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the Education Scotland Learning and Teaching Online.
- they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- They model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Learners/pupils

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement (this should include personal devices – where allowed)
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should avoid plagiarism and uphold copyright regulations
- will be expected to know and follow the school Online Safety Policy

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the digital technologies in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- providing them with a copy of the learners' acceptable use agreement (the school will need to decide if they wish parents/carers to acknowledge these by signature)
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, letters, website, learning platform and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- *reinforcing the online safety messages provided to learners in school*
- *the use of their children's personal devices in the school (where this is allowed)*

Community users

Community users who access school systems/website/learning platform as part of the wider school provision may be expected to sign a community user agreement before being provided with access to school systems. (A community user's acceptable use agreement template can be found in the appendices).

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the school's online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to senior leaders and the governing body.

The Online Safety Group has the following members (amend as appropriate):

- *online safety lead*
- *child protection/safeguarding lead*
- *senior leaders*
- *teacher and support staff members*
- *learners/pupils*
- *parents/carers*
- *community representatives*

Members of the Online Safety Group (or other designated group) will assist the Online Safety Lead (or other relevant person) with:

- the production/review/monitoring of the school Online Safety Policy/documents
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage of online safety within and across the curriculum
- reviewing network/filtering/monitoring/incident logs, where possible and appropriate
- encouraging the contribution of learners to staff awareness, recent trends and the school online safety provision
- consulting stakeholders – including staff/parents & carers about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe Scotland self-review tool.

Professional Standards

There is an expectation that national professional standards will be applied to online safety as in other aspects of school life i.e.

- there is a willingness to develop and apply new techniques/technologies to suit the purposes of intended learning in a structured and considered approach and to learn from the experience.
- practitioners are able to reflect on their practice, individually and collectively, against nationally agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

Online Safety Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they can use digital technologies responsibly, protecting themselves and the school and how they can use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels (to be described)
- *is published on the school website/social media page.*

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable Use Policies

An Acceptable Use Policy (AUP) is a document that outlines a school/local authority's expectations on the responsible use of technology by its users. In most schools they are signed or acknowledged by their staff as part of their conditions of employment. Some may also require learners and parents/carers to sign them, though it is more important for these to be understood and followed rather than just signed.

The Online Safety Policy and appendices define acceptable use at the school, including for the following groups:

- learners – differentiated by age. Learners will be introduced to the acceptable use rules at induction, the start of each school year and regularly re-enforced during lessons, assemblies and by posters/splash screens around the school. *Learner groups (to be described) are encouraged to suggest child friendly guidance of the rules.*
- staff and volunteers are made aware that their use of digital technologies is subject to a school/local authority AUP
- parent/carer agreements inform them of the expectations of acceptable use for their children and may seek permissions for digital images, the use of cloud systems etc.
- community users that access school digital technology systems may be required to sign an AUP.

The acceptable use agreements will be communicated/re-enforced through: (amend as appropriate)

- learner handbook
- staff induction and handbook
- splash screens
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website/social media
- peer support.

Schools will need to discuss and agree which activities are acceptable/unacceptable. This will vary with the size/structure of the school and the ages of the learners. It is recommended that the school should discuss and agree on these activities and to complete the following tables as guidance for members of the school community:

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post,	Any illegal activity for example: • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	• Encouraging or assisting suicide • Offences relating to sexual images i.e. revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering * N.B. Schools should refer to information in the National Guidance for Child Protection in Scotland 2021 about dealing with nudes and semi-nudes being shared (youth produced sexual imagery) and Education Scotland guidance on Responding to Sexual Behaviour of Young People..					
Users shall not undertake activities that might be classed as cyber-crime under the computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information here					
Users shall not undertake activities that are not illegal but are classed as unacceptable re school/council policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs.				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

	Staff and other adults	Learners

Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming								
Online shopping/commerce								
File sharing								
Social media								
Messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to school								
Use of mobile phones for learning at school								
Use of mobile phones in social time at school								
Taking photos on mobile phones/cameras								
Use of other personal devices, e.g. tablets, gaming devices								

Use of personal e-mail in school, or on school network/guest wi-fi								
Use of school e-mail for personal e-mails								

The school may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table.

When using communication technologies the school considers the following as good practice:

- the official school communication platforms may be regarded as safe and secure and are monitored. Users should be aware that all official communications are monitored. *Staff and learners should therefore use only the school approved communication platforms to communicate with others when in school, or on school systems (e.g. by remote access)*
- users must immediately report to the nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or social media must not be used for these communications. For guidance see GTCS guidance engaging online.pdf.*
- *learners should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of digital citizenship and the need to communicate appropriately when using digital technologies.*
- *Staff should be reminded about good practice in using social media re professional reputation*
- *relevant policies and permissions should be followed when posting personal information online e.g. school website and social media. Only official e-mail addresses should be used to identify members of staff and pupils.*

Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school child protection and safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.

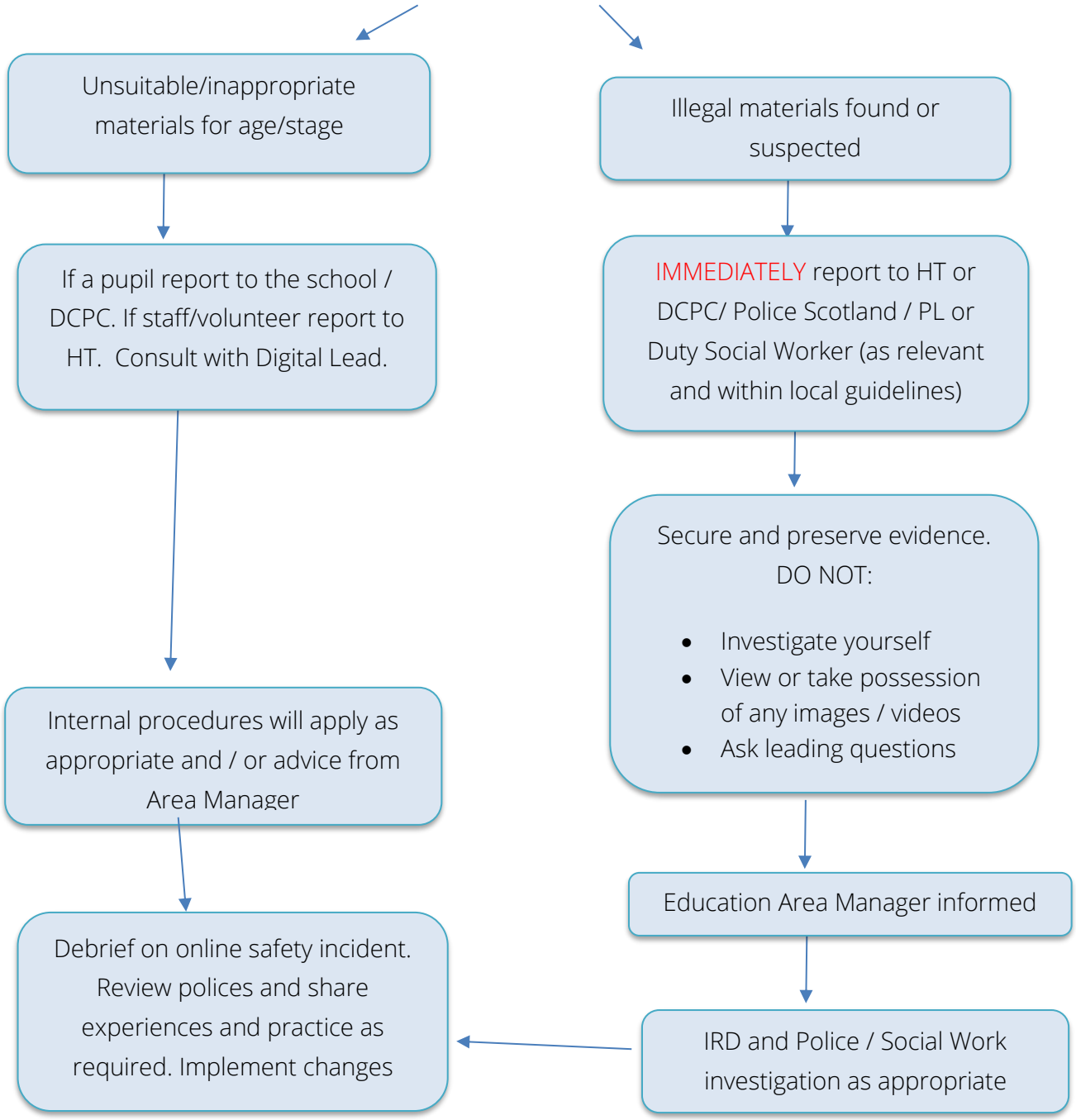
(Schools may wish to consider the use of online/anonymous reporting systems, which can be used by all members of the school community)

- all members of the school community will be made aware of the need to immediately report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Child Protection Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with the various risks related to online safety
- if there is any suspicion that the incident involves child abuse images, any other illegal activity or the potential for serious harm (see flowchart and user actions below), the incident must be escalated through the normal school child protection procedures and the police informed. In these circumstances any device or account involved should be isolated or suspended to support a potential police investigation. In addition to child abuse images such incidents would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials.
- any concern about staff misuse will be reported immediately to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the local authority
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g. peer support for those reporting or affected by an online safety incident
- incidents should be logged (insert details here). (A template reporting log can be found in the appendix, but many schools will use logs that are included with their management information systems (MIS).
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP;
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*

- *learners, through assemblies/lessons*
- *parents/carers, through newsletters, school social media, website*
- *local authority/external agencies, as relevant*

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

Online Safety Incident



At all times follow local and National Child Protection guidelines

National guidance for child protection in Scotland 2021 - gov.scot (www.gov.scot)

HT	Head teacher	DCPC	Designated Child Protection Coordinator
PL	Practice Lead from Family Teams	IRD	Interagency Referral Discussion

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows: (the school will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues. Schools have found it useful to use the charts below at staff meetings/training sessions)

Responding to Learner actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Principal Teacher / Deputy Head	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords									
Corrupting or destroying the data of other users.									
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature									

Unauthorised downloading or uploading of files or use of file sharing.									
Using proxy sites or other means to subvert the school's filtering system.									
Accidentally accessing offensive or pornographic material and failing to report the incident.									
Deliberately accessing or trying to access offensive or pornographic material.									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.									
Unauthorised use of mobile phone / digital camera / other mobile device, including taking images									
Unauthorised use of social media / messaging apps / streaming services / video broadcasting / gaming / personal e-mail									
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.									
Continued infringements of the above, following previous warnings or sanctions.									

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X				
Deliberate actions to breach data protection or network security rules.								
Deliberately accessing or trying to access offensive or pornographic material								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Using proxy sites or other means to subvert the school's filtering system.								
Unauthorised downloading or uploading of files or file sharing								
Breaching copyright or licensing regulations.								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.								
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature								
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers								

Inappropriate personal use of the digital technologies e.g. social media / personal e-mail								
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.								
Failing to report incidents whether caused by deliberate or accidental actions								
Continued infringements of the above, following previous warnings or sanctions.								

Education

Online Safety Education Programme

While regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and progressive, aligned with Curriculum for Excellence. Consideration should be made for delivering online safety education either discretely and/or embedded within an interdisciplinary learning approach.

Schools may wish to consider Project EVOLVE for this purpose. There should be opportunities for creative activities and will be provided in the following ways (statements may need to be adapted, depending on school structure and the age of the learners).

- a planned online safety curriculum across all year groups and a range of subjects, (e.g. RSHP, Technology, Health and Well-being) and topic areas and should be regularly revisited and evaluated
- the programme should build on prior knowledge and experience of pupils in order to ensure relevance and interest (see guidance on Project EVOLVE knowledge maps)
- key online safety messages should be enhanced by a planned programme of assemblies and tutorial/pastoral activities
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to all learners at different ages and abilities such as those with additional support for learning or those with English as an additional language. Learners considered to be at increased risk online are provided with targeted or differentiated online safety education
- learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- *Learners should be helped to understand the need for the acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school*
- *staff should act as good role models in their use of digital technologies, the internet and mobile devices*
- *in lessons where it is planned to use online resources, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- *where learners are allowed to freely search online, staff should be vigilant in supervising the learners and monitoring the content of the sites and services they visit*
- the online safety education programme will be regularly audited and evaluated to ensure the quality of learning and outcomes.

Contribution of Learners

The school acknowledges, learns from and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the

school community and how this contributes positively to the personal development of learners. Their contribution is recognised through: (amend as relevant)

- *mechanisms to seek learner feedback and opinion to inform online safety policy and practice*
- *appointment of digital leaders/anti-bullying ambassadors/peer mentors (or similar groups)*
- *the Online Safety Group has learner representation*
- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events for the wider school community e.g. parents' events/engagements, family learning programmes etc.*

Staff/volunteers

All staff receive online safety training/awareness and understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select/delete as appropriate)

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- *the Online Safety Lead and Child Protection Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. from the LA and other relevant organisations) and by reviewing guidance documents released by relevant organisations*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days*
- *the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.*

Parent Council

It is recommended that members of the Parent Council are offered regular online safety training/awareness raising, with a view to extending training/awareness to the wider parent forum.

Governors (in independent schools) should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding.

Parental Engagement

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will seek to provide information and awareness to parents and carers through: (select/delete as appropriate)

- *regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes*
- *regular opportunities for engagement with parents/carers on online safety issues through awareness workshops/parent/carer evenings etc*
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.*
- *letters, newsletters, website, learning platform*
- *high profile events/campaigns e.g. Safer Internet Day*
- *reference to the relevant web sites/publications,*
- *Sharing good practice with other schools in clusters and or the local authority about successful parental engagement strategies.*

Community and Stakeholder Engagement

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- providing family learning courses in use of new digital technologies and online safety
- online safety messages targeted towards families and relatives.
- the school will provide online safety information via their learning platform, website, and social media for the wider community

- *supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision (further self-review tools are available to support these groups – 360EarlyYears and 360Groups)*

The school welcomes the involvement of relevant external groups and agencies who are able to provide knowledge, training or services that enhance the school's online safety provision.

Technology

In local authority schools, the school should work with the local authority to ensure the technical security of the school's systems and users. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety, cyber-security and data protection.

Other schools (e.g. Independent Schools) may provide Technical Security solutions themselves or arrange these through an external organisation. The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection. Where external organisations are employed, it is important that the contractor is fully aware of the school Online Safety Policy/acceptable use agreements and the school has a Data Processing Agreement in place with them.

Filtering

- internet access is filtered for all users
- illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- there is an appropriate and balanced approach to providing access to online content according to role and/or need
- there are regular reviews of filtering logs to alert the school to breaches of the filtering policy, which are then acted upon.
- *differentiated user-level filtering is in place* (*allowing different filtering levels for different ages/stages and different groups of users: staff/learners, etc.)*

- *younger learners will use child friendly/age appropriate search engines e.g. SWGfL Swiggle*
- *where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school/local authority policy and practice.*
- *the system manages access to content through non-browser services/contextual filtering (e.g. apps and other mobile technologies)*

Monitoring

The school / local authority monitors all network use across all its devices and services.

An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored.

There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice

Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school / local authority protects users and school systems through the use of the appropriate blend of strategies strategy informed by risk assessments. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*
- *use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)*

Technical Security

The provision and control of digital infrastructure in the majority of Scottish schools will be the responsibility of respective local authorities. Schools should therefore work closely with their local authorities to amend statements as appropriate and ensure that relevant statements are complied with. Independent schools will

need to ensure that their technical security is ensured through their own internal and external arrangements and should amend the sections below as relevant to their circumstances.

The school will work closely with their local authority to ensure that the school's digital infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities. School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in local authority/other relevant body policy and guidance)

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of copies off-site or in the cloud, (this is good practice in helping to prevent loss of data from ransomware attacks)
- all users have clearly defined access rights to school technical systems and devices.
- all school networks and systems will be protected by secure passwords.
- all users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- the master account passwords for the school systems are kept in a physically secure place. It is recommended that these are secured using two factor authentication for such accounts (further guidance is available in the 'Technical Security policy template' in the Appendix)
- passwords should be long. Good practice highlights that passwords over 12 characters in length are more difficult to crack. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length is more secure than any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords/passphrases should be easy to remember, but difficult to guess or crack
- password requirements for learners should be age-appropriate should increase in complexity as learners progress through school
- Software licence logs are accurate and up-to-date and regular checks are made to reconcile the number of licences purchased against the number of software installations (inadequate licencing could cause the school/local authority to breach the Copyright Act which could result in fines or unexpected licensing costs)
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person
- appropriate security measures are in place (schools may wish to provide more detail which may need to be provided by the service provider) to protect the servers, firewalls, routers,

wireless systems, workstations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school/local authority systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date anti-virus software.

- an agreed policy is in place for the provision of temporary access of 'guests', (e.g. trainee teachers, supply teachers, visitors) onto the school systems
- an agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school
- an agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile technologies

Mobile technology devices may be school/local authority owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include:

- security risks in allowing connections to the school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction

- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

A more detailed mobile technologies policy template can be found in the Appendix. The school may however choose to include these aspects of their policy in a comprehensive acceptable use agreement, rather than in a separate mobile technologies policy. It is suggested that the school should in this overall policy document outline the main points from their agreed policy. A checklist of points to be considered is included below.

- The school acceptable use agreements for staff, learners, parents and carers outline the expectations around the use of mobile technologies.
- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems).

	School devices				
	School owned for individual use	School owned for multiple users	Authorised device[1]	Learner owned	Staff owned
Allowed in school				Yes/No[2]	Yes/No
Full network access (e.g. file systems)					
Internet only					
No network or internet access					

[1] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

[2] The school should add below any specific requirements about the use of mobile/personal devices in school.

Aspects that the school may wish to consider and include in their Online Safety Policy, mobile technologies policy or acceptable use agreements should include the following:

School owned/provided devices:

- *to whom they will be allocated*
- *where, when and how their use is allowed – times/places/in/out of school (n.b. the need for some areas to be clearly identified as mobile free zones)*
- *if personal use is allowed*
- *levels of access to networks/internet (as above)*
- *management of devices/installation of apps/changing of settings/monitoring*
- *network/broadband capacity*
- *technical support*
- *filtering of devices*
- *protection of devices and systems e.g. antivirus, anti-malware*
- *access to cloud services*
- *use on trips/events away from school*
- *data protection*
- *taking/storage/use of images*
- *exit processes, what happens to devices/software/apps/stored data if user leaves the school*
- *liability for damage*
- *staff training.*

Personal devices

- *which users are allowed to use personal mobile devices in school (staff/learners/visitors)*
- *restrictions on where, when and how they may be used in school*
- *if used in support of learning, how staff will plan their lessons around any potential variety of device models and different operating systems*
- *storage*
- *whether staff will be allowed to use personal devices for school business*
- *levels of access to networks/internet (e.g. access, or not, to internet/guest wi-fi/network)*
- *network/broadband capacity*
- *technical support (this may be a clear statement that no technical support is available)*
- *filtering of the internet connection to these devices and monitoring the access*
- *protection of devices and systems e.g. antivirus, anti-malware*
- *management of software licences for personally owned devices*

- *data protection*
- *taking/storage/use of images*
- *liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility)*
- *identification/labelling of personal devices*
- *how visitors will be informed about school requirements*
- *how education about the safe and responsible use of mobile devices is included in the school online safety education programmes*
- *how misuse will be dealt with*

Social media

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the relevant Professional Standards, but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published. This includes sharing information which could inadvertently identify someone.
- education/training being provided including acceptable use, age restrictions, social media, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- guidance for learners, parents/carers

School staff should ensure that:

- no reference should be made in personal social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school or local authority. Note that any online activities (posting, sharing, liking, group membership, who you follow etc.) have the potential to affect your professional reputation or your school's reputation (irrespective of whether posted in a personal capacity or in a private group).
- security settings on personal online profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of online communications technologies.

When official school social media accounts are established there should be:

- a process for approval by senior leaders
- clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *the school permits reasonable and appropriate access to private social media sites*

Monitoring of public social media

- As part of active social media engagement, the school will pro-actively monitor the Internet for public postings about the school
- the school should effectively respond to social media comments made by others according to a defined policy or process

- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Group to ensure compliance with relevant school policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

The social media policy template in Appendix C4 provides more detailed guidance on the school's responsibilities and on good practice.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

Should a school choose to use live-streaming or video-conferencing, headteachers and staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the Supporting Remote Learning guidance

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm (select/delete as appropriate):

- when using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images

- *staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images. Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes*
- *care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute*
- *learners must not take, use, share, publish or distribute images of others without their permission*
- *photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images*
- *learners' full names will not be used anywhere on a website or blog, particularly in association with photographs*
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. (See parents and carers acceptable use agreement in the Appendix). Permission is not required for images taken solely for internal purposes
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored on the school network in line with the school retention policy
- *learners' work can only be published with the permission of the learner and parents/carers.*

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through (amend as necessary):

- *Public-facing website*
- *Social media*
- *Online newsletters*
- *Other*

The school website is managed/hosted by (insert details). The school ensures that good practice has been observed in the use of online publishing e.g. use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is no risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected and full names are not published.

The school public online publishing provides information about online safety e.g. publishing the schools Online Safety Policy; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process

Cyber and Information Security

Local authority schools will be required to follow the data protection policies of their local authority, acting as the Data Controller. Other schools will need to ensure that as the Data Controller they will need to have their own data protection policy and relevant staff roles to meet their statutory requirements.

All schools should ensure that:

- They provide staff, parents, volunteers, and older children with information about how the school looks after their data and what their rights are in a Privacy Notice (in local authority schools this will be the local authority privacy notice)
- All staff are aware of the relevant Data Protection Policy (school or local authority)
- Staff receive training as relevant to ensure they understand and follow the requirements placed on them to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Staff can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Staff only use encrypted mobile devices (including USBs) for personal data, particularly when it is about children
- will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home (e.g. VPN access to the school network, or a work laptop provided).

The sections below will support schools that are required to have their own Data Protection Policy (i.e. not local authority schools).

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school:

- *has a Data Protection Policy. (see appendix for template policy)*
- *implements the data protection principles and is able to demonstrate that it does so*
- *has paid the appropriate fee to the Information Commissioner's Office (ICO)*
- *has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO*
- *has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it*
- *the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed*
- *has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it*
- *information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed*
- *will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this*
- *data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals*
- *has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them*
- *carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier*
- *IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners*
- *has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors*

- *understands how to share data lawfully and safely with other relevant data controllers.*
- *has clear and understood policies and routines for the deletion and disposal of data*
- *reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this it has a policy for reporting, logging, managing, investigating and learning from information risk incidents*

When personal data is stored on any mobile device or removable media the:

- data will be encrypted and password protected.
- device will be password protected. (be sure to select devices that can be protected in this way)
- device will be protected by up to date virus and malware checking software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g. online safety education, awareness and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this school Online Safety Policy template and of the 360 safe Scotland online safety self-review tool:

Appendices

A1 Learner Acceptable Use Agreement template – for Senior Phase
A2 Learner Acceptable Use Agreement Template – for P3 to S2
A3 Learner Acceptable Use Policy Agreement Template – for Nursery to P2
A4 Parent/Carer Acceptable Use Agreement Template and permission forms
A5 Staff (and Volunteer) Acceptable Use Policy Agreement Template
A6 Acceptable Use Agreement for Community Users Template
A7 Responding to incidents of misuse – flow chart
A8 Record of reviewing devices/internet sites
A9 Reporting Log
B1 Training Needs Audit Log
C1 Technical Security Policy Template (including filtering, monitoring and passwords)
C2 Personal Data Advice and Guidance
C3 Mobile Technologies Policy Template (inc. BYOD/BYOT)
C4 Social Media Policy Template
C5 Summary of Legislation

Links to other organisations or documents

Note: Schools/settings should check with their local authority guidance and policy prior to adopting the templates provided below.

A1 Learner Acceptable Use Agreement template – for Senior Phase

Sections that include advice or guidance are written in BLUE. It is anticipated that schools will remove these sections from their final acceptable use document. Schools should review and amend the contents of this agreement to ensure that it is consistent with their Online Safety Policy and other relevant school policies. Due to the number of optional statements and the advice/guidance sections included in this template, it is anticipated that the final document will be more concise. Schools will need to decide on the suitability of the agreement/statements/language used and may wish to amend these in light of the age/abilities of the learners.

School policy

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that children and young people will have good access to digital technologies, be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications and will act responsibly online
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will be aware of potential risks of communicating with people I don't know when online

- I will not publicly disclose or share personal information about myself or others when online (this could include names, addresses, e-mail addresses, passwords, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable to a trusted adult when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission (schools should amend this section to take account of their policy on each of these issues)
- I will not try (unless I have permission) to stream or download/upload data that might take up internet capacity and prevent other users from being able to carry out their work

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute digital video/images of anyone without gaining their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/tablets/laptops/gaming devices/smart devices etc.) in the school if I have permission (schools should amend this section in the light of their mobile devices policies). I understand that if I do use my own devices in the school I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- In accordance with school policy, I will immediately report, to the relevant staff member, any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in messages or any attachments to messages if I have any concerns about the validity of the message (due to the risk of the attachment containing viruses or other harmful programmes).

- I will not install or attempt to install or store unauthorised apps, software or extensions on any school device, nor will I try to alter approved device settings.
- I will only use social media sites with permission and at the times that are allowed (schools should amend this section to take account of their policy on access to social media).

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work, and will give appropriate credit to the creator
- where work is protected by copyright, I will not try to download copies (including music and videos)
- when I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school has the right to take action against me if I am involved in online incidents of inappropriate behaviour, when I am out of the school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) loss of access to the school network/internet, detentions, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.

The school will need to decide if they will ask learners (and/or) their parents/carers to sign the AUA or whether it is sufficient to just make it clear that these rules should be followed and to re-enforce them through the year. The form below is provided for those schools that wish to have them signed.

Learner Acceptable Use Agreement Form (optional)

This form relates to the learner acceptable use agreement; to which it is attached.

Please complete the sections below to confirm that you have read, understood and agree to the rules included in the learner acceptable use agreement. If you do not sign and return this agreement, access may not be granted to school systems. (Schools will need to decide if they require learners to sign, or whether they wish to simply make them aware through education programmes/awareness raising).

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, tablets, laptops, gaming devices, smart devices etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: .....

Group/Class: .....

Signed: .....

Date: .....

Parent/Carer Countersignature (optional)

It is for schools to decide whether or not they require parents/carers to sign the parent/carer acceptable use agreement (see template later in this document in the Parent/Carer AUA). This includes a number of other permission forms (including digital and video images/cloud-based services).

Some schools may, instead, wish to add a countersignature box for parents/carers to this learner acceptable use agreement.

A2 Learner Acceptable Use Agreement Template – for P3 to S2

Sections that include advice or guidance are written in BLUE. It is anticipated that schools will remove these sections from their final acceptable use document. Schools should review and amend the contents of this agreement to ensure that it is consistent with their school policies. Schools will need to decide on the suitability of the agreement/statements/language used and may wish to amend these in light of the age/abilities of the learners.

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, encourage creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and the internet, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of potential risks of communicating with people I don't know when online
- I will not share personal information about myself or others when online
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me

- I will immediately tell a trusted adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the approved settings on any devices or try to install any unauthorised software or apps.
- I will tell a trusted adult if a device is damaged or if anything else goes wrong.
- I will only use devices to do things that I am allowed to do. (schools may wish to add anything that would not be allowed e.g. online games, file sharing etc.)

I understand that I am responsible for my actions, both in and out of school: know that there are other rules that I need to follow:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and respectful when I communicate with others and I appreciate that others may have different opinions to me.
- I will not take or share digital videos/images of anyone without gaining their permission.

I know that there are other rules that I need to follow:

- I will only use my own personal devices (mobile phones/tablets/laptops/gaming devices/smart devices etc.) in the school if I have permission (schools should amend this section in the light of their mobile devices policies). If I am allowed, I still have to follow all the other school rules if I use them.
- I will only use social media sites with permission and at the times that are allowed (schools should amend this section to take account of their policy on access to social media).
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When searching online, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work and give appropriate credit to the creator.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) *loss of access to the school network/internet, detentions, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.*

The school will need to decide if they will ask learners (and/or) their parents/carers to sign the AUA or whether it is sufficient to just make it clear that these rules should be followed and to re-enforce them through the year. The form below is provided for those schools that wish to have them signed.

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access may not be granted to school systems. (Schools will need to decide if they require learners to sign, or whether they wish to simply make them aware through education programmes/awareness raising).

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices
- I use my own devices in the school (when allowed) e.g. mobile phones, tablets, laptops, gaming devices, smart devices etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: ..... Group/Class: .....

Signed: ..... Date: .....

Parent/Carer Countersignature (optional)

It is for schools to decide whether or not they require parents/carers to sign the parent/carer acceptable use agreement (see template later in this document in the Parent/Carer AUA). This includes a number of other permission forms (including digital and video images/cloud-based services).

Some schools may, instead, wish to add a countersignature box for parents/carers to this learner acceptable use agreement.

A3 Learner Acceptable Use Policy Agreement Template – for Nursery to P2

Sections that include advice or guidance are written in BLUE. It is anticipated that schools will remove these sections from their final acceptable use document. Schools should review and amend the contents of this agreement to ensure that it is consistent with their school policies. Schools will need to decide on the suitability of the agreement/statements/language used and may wish to amend these in light of the age/abilities of the learners.

This is how we stay safe when we use digital devices:

- I will ask a teacher or trusted adult if I want to use a digital device.
- I will only use a device for activities that the teacher or trusted adult allow me to do.
- I will take care of all devices.
- I will ask for help from a teacher or trusted adult if I am not sure what to do or if I think I have done something wrong when using a device.
- I will tell a teacher or trusted adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a device.

Signed (child): .....

(The school/setting will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent/carer should be sufficient)

Signed (parent): .....

Schools/settings using this acceptable use agreement for younger children may also wish to use (or adapt for use) the parent/carer acceptable use agreement (the template can be found later in these templates) as this provides additional permission forms (including the digital and video images permission form).

A4 Parent/Carer Acceptable Use Agreement Template and permission forms

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while online and using digital devices
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that learners have access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the learners in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work. (Schools will need to decide whether or not they wish parents to sign the acceptable use agreement on behalf of their child)

Permission Form

Parent/Carers Name:..... Name(s) of Learners.....

As the parent/carer of the above learners, I acknowledge and understand the acceptable use policy and understand my responsibility to ensure my child remains safe when online and using digital devices.

I understand that the school has discussed the acceptable use agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of the school.

I understand that the school/local authority takes every reasonable precaution, including monitoring and filtering systems, to ensure that young people are safe when they are online and using digital

devices. I understand that due to the ever-changing nature of online content, filtering and monitoring systems may not always be successful in preventing access to all inappropriate content.

I understand that my child's online activity on school systems/devices will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use online at home and will inform the school if I have concerns over my child's online safety.

Signed: .....

Date: .....

Use of Digital/Video Images

Local authority schools are likely to collect this information through the agreed MIS (SEEMiS) forms. The template below is available for use by other schools, as appropriate.

We take photographs/videos of the children for the purposes of recording and tracking pupil progress and compiling evidence for assessment purposes. These are kept in secure locations within the school and destroyed in line with our retention policy. We may also need to share these files with third parties, such as [*Insert professionals/third parties who may be a recipient or contributor, if any*]. Further details can be found in the privacy notice.

On other occasions the school may wish to publish photographs and/or video footage of pupils in public documents such as the school prospectus, our social media pages (e.g. Twitter) and website, on display around the school, and in community publications such as local newspapers. All images are published with the strictest regard for safeguarding and child protection, and only with your consent.

The school will comply with data protection laws and request parent's/carer's permission before publishing images of members of the school. We will also ensure that when images are published the learner cannot be identified using their names.

Please note that you can withdraw your consent at any time. If you have any queries or wish to withdraw or review your consent, please contact the school.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act 2018). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

Digital/Video Images Permission Form

Parent/Carers Name:..... Name(s) of Learner(s):.....

Description of the use of Photographs or Images	Please Tick	
I agree for photographs/videos to be taken of my child during school activities for use on display boards or walls around the school.	☐ Yes	☐ No
I agree for photographs/videos to be taken of my child during school activities for use within school printed publications.	☐ Yes	☐ No
I agree for photographs/videos to be taken of my child during school activities for use on school digital channels (e.g. websites, social media).	☐ Yes	☐ No
I agree for photographs/videos to be taken of my child during school activities and used in local or national media (e.g. newspapers or television appearance).	☐ Yes	☐ No

OR

I do not wish any photographs/videos to be taken of my child for the purposes outlined above.	☐ Yes	☐ No

Signed: .....

Date: .....

Use of Cloud Systems

Schools that use cloud hosting services should assess the risk of sharing personal data with any other third party and should identify the correct lawful basis for this data sharing. It is likely that parent/carer consent may be required in order to create an account. Schools should consider the impact of relying on consent as the lawful basis if the service is regarded as essential to providing education. If consent is withdrawn and access to the service no longer possible, the school should consider if this would have a negative impact on the learners' education?

Local authority schools should liaise with their LA Data Officer / ICT Support for further guidance.

Schools may wish to include a simple form to collect any necessary permission here.

Learner Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the learner acceptable use agreement.

It is suggested that when the learner AUA is written that a copy should be attached to the parents/carers acceptable use agreement to provide information for parents and carers about the rules and behaviours that learners have committed to by signing the form.

A5 Staff (and Volunteer) Acceptable Use Policy Agreement Template

Sections that include advice or guidance are written in BLUE. It is anticipated that schools will remove these sections from their final document. Schools should review and amend the contents of this agreement to ensure that it is consistent with their Online Safety Policy and other relevant school policies. Due to the number of optional statements and the advice/guidance sections included in this template, it is anticipated that the final AUA will be more concise.

Local authority schools should use any LA agreement that is required.

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. Online and digital technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also allow staff to be more creative and productive in their work. All users should have an entitlement to safe online access.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe online and while using communications technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the school/local authority systems and users at risk
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the children and young people in my care in the safe use of digital technology and embed online safety in my work with children and young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, tablets, e-mail, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of the school (schools should amend this section in the light of their policies which relate to the use of school systems and equipment out of the school)
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published online it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with learners and parents/carers. Staff should be made aware of the risks attached to using their personal e-mail addresses/mobile phones/social networking sites for such communications)
- I will not engage in any online activity that may compromise my professional responsibilities, as outlined in the GTCS Professional Standards.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. (schools should amend this section in the light of their policies which relate to the use of staff devices)
- I will not use personal e-mail addresses on the school systems. (schools should amend this section in the light of their e-mail policy – some schools will choose to allow the use of staff personal e-mail addresses on the premises).
- I will not open any hyperlinks in e-mails or any attachments to e-mails, unless the source is known and trusted, or if I have any concerns about the validity of the e-mail (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might impact network capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. (schools should amend this section in the light of their policies on installing programmes/altering settings)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in the school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to the local authority / other relevant agencies and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

A6 Acceptable Use Agreement for Community Users Template

Local authority schools should use any LA agreement that is required.

This acceptable use agreement is intended to ensure that:

- community users will be responsible and stay safe while using school systems and devices and will be protected from potential harm in their use
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might impact network capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have explicit permission to do so.

- I will not disable/cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report equipment/software damage/faults, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- I will not download or distribute copies of work protected by copyright (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

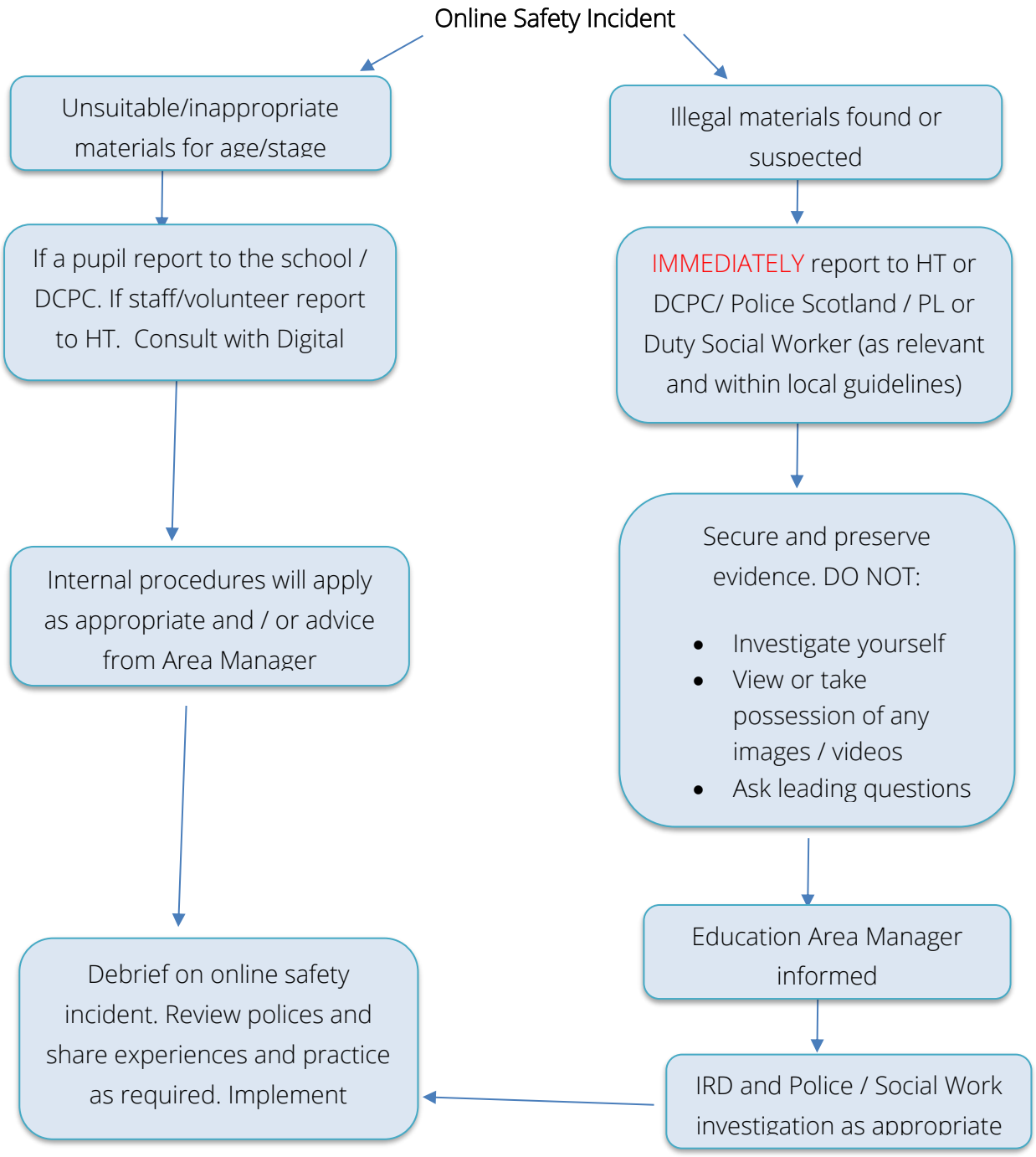
I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Name: .....

Signed: .....

Date: .....

A7 Responding to incidents of misuse – flow chart



At all times follow local and National Child Protection guidelines

National guidance for child protection in Scotland 2021 - gov.scot (www.gov.scot)

HT	Head teacher	PL	Practice Lead from Family Teams
DCPC	Designated Child Protection Coordinator	IRD	Interagency Referral Discussion

A8 Record of reviewing devices/internet sites

(responding to incidents of misuse)

School: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of device used for review

.....

.....

Date	Web address / app / device	Reason for concern

Conclusion and action proposed or taken

A9 Reporting Log

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

B1 Training Needs Audit Log

School: .....

Relevant training in the last 12 months	Identified Training Need	To be met by	Cost	Review Date

C1 Technical Security Policy Template (including filtering, monitoring and passwords)

This policy is for use by schools where local authority policy is not mandated.

Local authority schools should use their local authority policy as stipulated.

Suggestions for use

Within this template sections which include information or guidance are shown in BLUE. It is anticipated that schools would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

Where sections in the template are written in italics it is anticipated that schools would wish to consider whether or not to include that section or statement in their completed policy.

Where sections are highlighted in BOLD text, it is the view of the SWGfL Online Safety Group that these would be an essential part of a school Online Safety Policy.

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school systems
- there is oversight from senior leaders and these have impact on policy and practice.

If the school has a managed service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that might otherwise be carried out by the school itself (as suggested below). It is also important that the

managed service provider is fully aware of the school Online Safety Policy/acceptable use agreements).

Responsibilities

The management of technical security will be the responsibility of (insert title) (schools will probably choose the Network Manager/Technical Staff/Head of Computing or other relevant responsible person)

Technical Security

Policy statements

The school will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements (if not managed by the local authority, these may be outlined in local authority/other relevant body technical/Online Safety Policy and guidance)
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling must be securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (this may be at school, local authority or managed provider level)
- all users will have clearly defined access rights to school technical systems. *Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually, by the Online Safety Group.*
- users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security (see password section below)
- (insert name or role) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)

- *mobile device security and management procedures are in place* (where mobile devices are allowed access to school systems). (schools may wish to add details of the mobile device security procedures that are in use).
- *school/local authority/managed service provider/technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement*. (schools may wish to add details of the monitoring programmes that are used)
- *remote management tools are used by staff to control workstations and view users' activity*
- *an appropriate system is in place* (to be described) *for users to report any actual/potential technical incident to the Online Safety Lead/network manager/technician (or other relevant person, as agreed)*
- an agreed policy is in place (to be described) for the provision of temporary access of "guests", (e.g. probationary teachers, supply teachers, visitors) onto the school system
- *an agreed policy is in place* (to be described) *regarding the downloading of executable files and the installation of programmes on school devices by users*
- *an agreed policy is in place* (to be described) *regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school*
- an agreed policy is in place (to be described) regarding the use of portable media and cloud services by users on school devices (see school personal data policy template in the appendix for further detail)
- the school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see school personal data policy template in the appendix for further detail)

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, e-mail and learning platform). Where sensitive data is in use – particularly when accessed on mobile devices – schools may wish to use more secure forms of authentication e.g. two step verification.

Further guidance can be found from the National Cyber Security Centre and SWGfL "Why password security is important"

Policy Statements:

- These statements apply to all users.
- All school networks and systems will be protected by secure passwords.

- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other designated person) and will be reviewed, at least annually, by the Online Safety Group (or other group).
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by xxxxx (insert name or title) (see section on password generation in technical notes) who will keep an up to date record of users and their usernames.

Password requirements:

- Passwords should be long. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of the school
- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system
- The process for resetting passwords should be easily understood and accessible
- *The school may wish to recommend to staff and learners (depending on age) that they make use of a 'password manager' these can store passwords in an encrypted manner and can generate very difficult to crack passwords. There may be a charge for these services.*
- *Passwords should not be set to expire as long as they comply with the above, but should be unique to each service the user logs into.*

Learner passwords:

Primary schools will need to decide at which point they will allocate individual usernames and passwords to learners. They may choose to use class logons for nursery to P2 (though increasingly children are using their own passwords to access programmes). Schools need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the acceptable use policy agreement. Use by learners in this way should always be supervised and members of staff should never use a class log on for their own network/internet

access. Schools should also consider the implications of using whole class/generic logins when providing access to learning environments and applications, which may be used outside school.

- Consideration should be made on how to securely store records of nursery to P2 learners' logins. Paper-based records are discouraged. Password management should allow users to reset their passwords electronically.
- Password length/complexity could be reduced where applicable in nursery to P2 phase or for children with additional support needs. Where external systems have different password requirements the use of random words or sentences should be encouraged.
- Password requirements for learners at P3 and above should increase as learners progress through school.
- Users will be required to change their password if it is compromised.
- Learners will be taught the importance of password security. This should include how passwords are compromised, and why these password rules are important (Project Evolve provides educational materials including 'Passwords').

Notes for technical staff/teams

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration should also be given to using two step verification for such accounts.
- An administrator account password for the school systems should also be kept in a secure place e.g. school safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account. (A school should never allow one user to have sole administrator access)
- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.
- *It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.*
- *Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated* by xxxxx (insert title) (schools may wish to have someone other than the school's technical staff carrying out this role e.g. an administrator who is easily accessible to users). *Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary and the user should be forced to change their password on first login. The generated passwords should also be long and random.*
- *Where automatically generated passwords are not possible, then a good password generator should be used by* xxxxx (insert title) *to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login.*
- *Requests for password changes should be authenticated* by (the responsible person) *to ensure that the new password can only be passed to the genuine user* (the school will need to decide

how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a learner)

- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expire after use. *(For example, your technical team may provide pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)*
- In good practice, the account is "locked out" following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).

Training/Awareness:

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users. It is also essential that users be taught how passwords are compromised, so they understand why things should be done a certain way.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's Online Safety Policy and technical/password security policy
- through the acceptable use agreement

Learners will be made aware of the school's password policy:

- in lessons (the school should describe how this will take place)
- through the acceptable use agreement

Parents/Carers will be made aware of the school's password policy:

- through the acceptable use agreement
- login screen
- through school communication channels

Audit/Monitoring/Reporting/Review:

The responsible person (insert title) will ensure that full records are kept of:

- User Ids and requests for password changes
- *User logins*
- *Security incidents related to this policy*

Filtering

Introduction

Filtering provides an important means of preventing users from accessing online material that is illegal, or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is important, therefore, to understand that filtering is only one

element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Many users are not aware of the flexibility provided by many filtering services at a local level for schools. Where available, schools should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

Schools need to consider carefully the issues raised and decide:

- Whether they will use the provided filtering service without change or to allow flexibility for sites to be added or removed from the filtering list for their organisation
- Whether to introduce differentiated filtering for different groups/ages of users
- Whether to remove filtering controls for some online activities e.g. social media at certain times of the day or for certain users
- Who has responsibility for such decisions and the checks and balances put in place
- What other system and user monitoring systems will be used to supplement the filtering system and how these will be used

Guidance on appropriate filtering and monitoring can be found on the UK Safer Internet Centre site.

Schools may wish to test their filtering for protection against illegal materials at: SWGfL Test Filtering

Responsibilities

The responsibility for the management of the school's filtering policy will be held by (insert title). They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must (schools should choose their relevant responses):

- be logged in change control logs
- be reported to a second responsible person (insert title):
- *either… be reported to and authorised by a second responsible person prior to changes being made* (recommended)
- *or… be reported to a second responsible person* (insert title) *every X weeks/months in the form of an audit of the change control logs*
- *be reported to the Online Safety Group every X weeks/months in the form of an audit of the change control logs*

All users have a responsibility to report immediately to (insert title) any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any apps or services that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

Online access is filtered for all users. Differentiated access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- *Either - The school maintains and supports the managed filtering service provided by the Internet Service Provider* (or other filtering service provider)
- *Or – The school manages its own filtering service* (N.B. If a school decides to remove the external filtering and replace it with another internal filtering system, this should be clearly explained in the policy and evidence provided that the Headteacher would be able to show, in the event of any legal issue that the school was able to meet its statutory requirements to ensure the safety of staff/learners)
- *The school has provided enhanced/differentiated user-level filtering through the use of the* (insert name) *filtering programme. (allowing different filtering levels for different ages/stages and different groups of users – staff/learners etc.)*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).*
- *Mobile devices that access the school network (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *Any filtering issues should be reported immediately to the filtering provider.*
- *Requests from staff for sites to be removed from the filtered list will be considered by the technical staff* (insert name or title) (N.B. an additional person should be nominated – to ensure protection for the Network Manager or any other member of staff, should any issues arise re unfiltered access). *If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.*

Education/Training/Awareness

Learners will be made aware of the importance of filtering systems through the online safety education programme (schools may wish to add details). They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through: (amend as relevant)

- the acceptable use agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc. (amend as relevant)

Changes to the Filtering System

In this section the school should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering (whether this is carried out in the school or by an external filtering provider)
- the grounds on which they may be allowed or denied (schools may choose to allow access to some sites e.g. social networking sites for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).
- how a second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records/audit of logs)
- any audit/reporting system

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to (insert title) who will decide whether to make school level changes (as above).

Monitoring

Some schools supplement their filtering systems with additional monitoring systems. If this is the case, schools should include information in this section, including – if they wish – details of internal or commercial systems that are in use. They should also ensure that users are informed that monitoring systems are in place.

No filtering system can guarantee 100% protection against access to unsuitable online content. The school will therefore monitor the activities of users on the school network/equipment as indicated in the school Online Safety Policy and the acceptable use agreement. *Monitoring will take place as follows:* (details should be inserted if the school so wishes).

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to: (schools should amend as relevant)

- the second responsible person (insert title)
- Online Safety Group
- External filtering provider/local authority/Police on request

This policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring/disciplinary action might be necessary).

Further Guidance

Schools may wish to seek further guidance. The following is recommended:

UKSIC - "Appropriate Filtering and Monitoring"

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: SWGfL Test Filtering

C2 Personal Data Advice and Guidance

This guidance is for use by schools where local authority guidance/policy is not mandated.

Local authority schools should use their local authority guidance/policy as stipulated.

Suggestions for use

This document is for advice and guidance purposes only. It is anticipated that schools will use this advice alongside their own data protection policy. This document is not intended to provide legal advice and the school is encouraged to seek their own legal counsel when considering their management of personal data.

What is personal data?

Personal data is "any information relating to an identified or identifiable natural person ('data subject')". An identifiable natural person is one who can be identified, directly or indirectly, by reference to:

- an identifier such as a name, an identification number, location data, an online identifier or
- to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Some types of personal data are known as 'special categories of personal data' and include the following:

"racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

The school/local authority must identify both a lawful basis (Article 6 of the GDPR) and a separate condition for processing special category data (Article 9 of the GDPR). These should be decided prior to any processing taking place, and further guidance is available on the Information Commissioner's Office (ICO) website

The ICO's powers are wide ranging in the event of non-compliance and schools must be aware of the huge impact that a fine or investigation will have on finances and also in the wider community for example in terms of trust.

The Data Protection Law sets out that a data controller must ensure that personal data shall be:

a) processed lawfully, fairly and in a transparent manner;
b) collected for specified, explicit and legitimate purposes ("purpose limitation");
c) adequate, relevant and limited to what is necessary ("data limitation");
d) accurate and, where necessary, kept up to date;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation"); and
f) processed in a manner that ensures appropriate security of the personal data

An overall principle of accountability requires the school/local authority to be responsible for and demonstrate compliance with data protection law.

Data protection law requires the school/local authority to always have a lawful basis for processing personal data. These can be summarised as:

(a) Consent:	the data subject has given clear consent for you to process their personal data for a specific purpose (see below for further guidance)
(b) Contract:	the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation:	the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests:	the processing is necessary to protect someone's life.
(e) Public task:	the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests:	the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

No single basis is 'better' or more important than the others and which basis is most appropriate to use will depend on your purpose and relationship with the data subject.

Data Mapping to identify personal data, data subjects and processing activities

The school and its employees will collect and/ or process a wide range of information concerning numerous data subjects and some of this information will include personal data. Further, the school may need to share some personal data with third parties. To be able to demonstrate and plan compliance and it is important that the school has a data map of these activities. These inform privacy notices and help put security measures in place to keep personal data secure, including steps to avoid a breach, and ensure Data Processing Agreements (i.e. contracts) are in place with the suppliers or contractors.

The data map should identify what personal data is held in digital format or on paper records in a school, where the information is stored, why it is processed, and how long it is retained.

In a typical data map for a school, the data subjects and personal data will include, but is not limited to:

- Parents, legal guardians, personal data of names, addresses, contact details
- Learners: curricular / academic data (e.g. class lists, learner progress records, reports, references, contact details, health and SEN reports)
- Staff and contractors: professional records (e.g. employment history, taxation and national insurance records, appraisal records and references, health records)

The ICO have advice and guidance on keeping a Record of Processing Activities.

The school/local authority will need to identify appropriate lawful process criteria for each type of personal data, and if this is not possible, such activities should be discontinued.

A school/local authority can use the public task lawful basis if processing takes place to perform an official task as set down in UK law:

"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" (Article 6(1)(e) of the GDPR)

If not, the school/local authority should consider each of the other lawful bases for processing in turn to assess how they fit with the processing and relationship with the data subject. As a public authority, please remember that legitimate interests cannot be used as a lawful basis when processing personal data to perform an official task or a public function.

The rules around consent should be considered carefully, as another lawful basis may be more appropriate. GDPR sets a high standard for consent and should put individuals in charge. Consent is now defined as:

"in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data".

This means that consent must be freely given, specific, informed, and an unambiguous indication of wishes by a statement or affirmative action. As a result, consent forms should be clear and concise; include an opt-in, granular approach; as well as explain why information is collected and how it will be processed to inform individuals. Implied consent is no longer suitable.

The DPA2018 modifies the GDPR so that the minimum age for consent to be obtained from a child is lowered to 13 years old.

The Information Commissioner's Office (ICO) gives clear advice on when it's appropriate to use consent as a lawful base. It states:

"Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."

The school should only use consent if none of the other lawful bases are appropriate. If you do so, you must be able to cope with people saying no (and/or changing their minds). Therefore, it's important that you only use consent for optional extras, rather than for core information the school requires in order to carry out its function. The below are examples where consent may or may not be appropriate;

- consent should be obtained when publishing a child's photo in any way (i.e. a school website, newsletter, prospectus, or social media).
- the school is required to hold learner and parent/carer details in an MIS. Therefore, it would not be appropriate to rely on consent, as the individual(s) would then have the right to opt out of the processing. In this case, the school could apply the public task lawful basis.
- The school is required to share information for the purposes of child protection issues. As a result, it would not be appropriate to rely on consent, as the individual(s) would have the right to opt out of the processing. The school could also alert an individual about an allegation made against them. In this case, the school could apply the public task lawful basis.

Content of Privacy Notices

Privacy Notices are a key compliance requirement as they ensure that each data subject is aware of the following points when data is collected/ processed by a data controller:

- the identity and contact details of the data controller
- what categories of personal data are being processed
- the purposes and lawful basis for processing the personal data
- where and how the personal data was sourced
- to whom the personal data may be shared with
- whether any personal data is transferred to a country outside of the EEA
- how long the personal data will be stored and retained
- the contact details of the Data Protection Officer
- the existence of automated decision making, including profiling
- data subject's rights and how to exercise them
- details of how to make a complaint to the school or ICO

The right to be informed is closely linked to the fair processing and transparency requirements of data protection principles. In order to comply, the school must provide parents/carers and learners with the above information when collecting personal data from individuals and ensure a privacy notice is easily accessible throughout the processing. For example, privacy notices could be passed to parents/carers and learners in the school prospectus, newsletters, or a specific letter/communication. The school could publish privacy notices on the school website. Parents/carers and learners who are new to the school should be provided with the privacy notice through an appropriate mechanism. Please be aware, however, that different forms of processing require a Privacy Notice, such as when processing visitor information or using personal data for employment purposes.

A school should ensure that privacy notices are available for learners as data subjects. Children and young people have the same rights as adults when it comes to their personal data. These include the rights described below and policies that explain this should be clear and age appropriate.

Data subject's right of access

Data subjects have a number of rights in connection with their personal data, which include:

- Right to be informed how personal data is collected, stored, managed, protected, and processed.
- Right of access to request a copy of personal information held of yourself. However, please be aware that information can sometimes be legitimately withheld.
- Right to rectification of inaccurate or incomplete personal data.
- Right to erasure where you have the right to have your personal data erased in certain circumstances. This does not include any personal data that must be retained by law.

- Right to restriction, which allows you to limit the way we use your personal data in some circumstances.
- Right to portability gives an individual the right to receive copies of data provided to a controller in a portable format.
- Right to object to the processing of one's personal data.
- Rights in relation to automated decision making and profiling.

Several of these are likely impact schools, such as the right of access. Therefore, the school should put procedures in place to deal with Subject Access Requests and other individual rights requests (e.g. erasure and rectification).

Subject Access Requests are probably the most common individual right request made to any organisation. These are written or verbal requests to access all or a part of the personal data held by the Data Controller in connection with a living individual. Controllers have one calendar month to provide the information, unless the case is unusually complex and an extension can be obtained.

Schools/local authorities must consider all information requested for disclosure. However, there are instances where personal data must not be disclosed to the applicant, even if requested:

- the personal data of any third parties (not relating to the data subject)
- if doing so would cause serious harm to the individual
- child abuse data
- adoption records
- Individual Development Plans for learners with Additional Learning Needs (ALN)

Your school/local authority must provide the information free of charge. However, there are occasional instances where a reasonable fee can be charged, for example if the request is clearly unfounded, or excessive.

Personal data breaches and how to manage them

Schools are "data rich" and hold a large volume of personal data on the learners in their care. This data can be in paper (i.e. manual records) and electronic format (e.g. shared drives, electronic databases, and Cloud solutions). Personal data is increasingly being held digitally with the introduction of electronic storage solutions (e.g. Google Drive) and the digital transfer or sharing of information. As a result, personal data is more accessible and the potential for data loss has increased significantly, especially where staff are working from remote locations (such as at home, other schools, or even public spaces).

Data protection law applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, this document will place emphasis on data that is held or transferred digitally due to being part of an overall Online Safety Policy template.

A personal data breach is described as a *"breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*. As a result, there is more to a personal data breach than simply losing personal data, and breaches can be the result of both accidental and deliberate causes. For example, a breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff or a pupil, accidental loss of equipment or paper records, or equipment failure.

An important part of managing a personal data breach is for the school/local authority to have a clear and well understood procedure for reporting breaches so they can implement actions and minimise any further risk. The school/local authority should have a policy for reporting, logging, managing and recovering from incidents, which establishes:

- a "responsible person" for reporting and investigating incidents
- how to manage personal data breaches, including an escalation procedure
- criteria for determining incident level and timescales, which should help to:

The school may find it useful to develop an incident report form template for staff to complete if a personal data breach is discovered. These forms support the school to record all the information required to analyse the incident and comply with the accessibility principle. An example form should include the following.

All 'high risk' breaches must be reported to the Information Commissioner's Office through the DPO based upon the school/local authority procedure for reporting incidents. Data protection laws require this notification to take place within 72 hours of becoming aware of the breach (where feasible).

Schools must consider whether an incident discovered poses a risk to the individuals (i.e. data subjects) involved, including the likelihood and severity of any risk to people's rights and freedoms. If the assessment suggested a high risk is unlikely, the incident does not need to be reported. However, there is a legal duty under data protection law to document the facts relating to a breach, its effects, and the remedial action taken by the organisation. The school/local authority should, therefore, maintain a log of all incidents.

Data Protection Impact Assessments (DPIAs)

Data Protection Impact Assessments (DPIAs) identify and assess privacy risks early on in a project that processes personal data to enable the school to mitigate them before the project launches.

DPIAs should be carried out by project leads under the support and guidance of the DPO. Schools/local authorities should conduct a DPIA before processing activity starts and run alongside the planning and development process.

- Step 1: Identify the need for using personal data
- Step 2: Describe the information flows
- Step 3: Identify the privacy and related risks
- Step 4: Identify privacy solutions
- Step 5: Sign off and record the DPIA outcomes
- Step 6: Integrate the DPIA outcomes back into the project plan

Data protection law requires a DPIA to be completed where processing is likely to result in a high risk to the rights and freedoms of individuals and for the below types of processing:

1. Systematic and extensive profiling with significant effects
2. Large scale use of sensitive data (i.e. special category or criminal data)
3. Public monitoring (i.e. CCTV)

For more information about DPIAs, please see this guidance on the ICO website.

A DPIA should contain the following:

- a description of the processing and the purpose
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals
- the measures in place to address risk, including security and to demonstrate that you comply.

And could be laid out in this way:

Describe source of risk and potential impact on individuals	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant, or severe	**Overall risk** Low medium high*	**If medium or high, options to reduce or eliminate risk**	**Effect on risk** Eliminated, reduced, or accepted	**Residual risk** Low medium high*	**Measure approved** yes/no

A DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

Secure storage of and access to data

The school/local authority should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and those processing personal data will be assigned appropriate access. For example, access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Good practice suggests that all users will use strong passwords. User passwords must never be shared.

Personal data may only be accessed on devices that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All data must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

School personal data should only be stored on school systems and devices. Personal devices (i.e. owned by the users) must not be used for the storage of school personal data.

When personal data is stored on any portable device/media or cloud service:

- The data must be encrypted and password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school/local authority policy once it has been transferred or its use is complete.

The school/local authority will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school/local authority should have a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school systems, including off-site backups.

Clear policies and procedures should be in place for the use of "Cloud Based Storage Systems" (e.g. Dropbox, Microsoft 365, Google Drive). Please be aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school must ensure that it is satisfied with controls put in place by remote/cloud-based data services providers to protect the data.

As a Data Controller, the local authority (or independent school) is responsible for the security of any data passed to a "third party". Specific data processing clauses must be included in all contracts where personal data is likely to be passed to a third party, for example apps or learning resources such as SeeSaw or Sumdog. These require a Data Processor that is processing personal data on behalf of the local authority/school to:

- only act on the written instructions of the local authority/school
- ensure that staff processing the personal data are subject to a duty of confidence
- take appropriate measures to ensure the security of processing
- only engage sub-processors with the prior consent of the controller, and under a written contract
- assist the controller in providing subject access to information and allowing data subjects to exercise their rights under the GDPR
- assist the controller in meeting its data protection obligations in relation to the security of processing, including the notification of personal data breaches and carrying out Data Protection Impact Assessments (DPIA)
- delete or return all personal data to the controller as requested at the end of the contract or as appropriate
- provide the controller with whatever information it needs to ensure that they are both meeting their data protection obligations
- tell the controller immediately if it is asked to do something infringing the GDPR, Data Protection Act 2018, or other applicable data protection law

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school or transferred to the local authority or other agencies. In these circumstances:

- Users may not remove or copy sensitive/restricted/protected personal data from the school or authorised premises without permission. Media should be encrypted and password protected and transferred securely for storage in a secure location.
- Users must take particular care that devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- Secure remote access to a management information system or learning platform is preferable when personal data (particularly special categories of personal data) is required by an authorised user from outside the organisation's premises (e.g. by a member of staff to work from their home). If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is stored in another country and advice should be sought from the Data Protection Officer in this event.

Disposal of personal data

The school/local authority should implement a retention schedule that defines the length of time personal data is held before secure destruction. The school/local authority must ensure the safe disposal of personal data when it is no longer required. Advice should be sought from the Data Protection Officer.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

A record of disposal log (i.e. Schedule for Disposal/Destruction) should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Demonstrating Compliance - Audit Logging / Reporting / Incident Handling

Local authorities/schools are required to keep records of processing activity. The data map referred to above will assist here. Records must include:

- the name and contact details of the data controller
- where applicable, the name and contact details of the joint controller and Data Protection Officer (DPO)

- the purpose of the processing
- to whom the data has been/will be disclosed
- description of data subject and personal data
- where relevant the countries it has been transferred to
- under which condition for processing the personal data has been collected
- under what lawful basis processing is being carried out
- where necessary, how it is retained and destroyed
- a general description of the technical and organisational security measures.

In order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore, local authority/school audit logs will need to be kept to:

- provide evidence of the processing activity and the DPIA
- record where, why, how and to whom personal data has been shared
- log the disposal and destruction of the personal data
- enable the school to target training at the most at-risk data
- record any breaches that impact on the personal data

Data Protection Fee

Local authorities/independent schools are required to pay the relevant annual fee to the Information Commissioner's Office (ICO) by law. This means the local authority/school is breaking the law if, as a data controller, it processes personal data and have either not paid a fee, or not paid the correct fee.

Responsibilities

Every independent school is required to appoint an independent Data Protection Officer (DPO) as a core function of 'the business'

The Data Protection Officer (DPO) can be internally or externally appointed.

They must have:

- expert knowledge
- timely and proper involvement in all issues relating to data protection
- the necessary resources to fulfil the role
- access to the necessary personal data processing operations
- a direct reporting route to the highest management level.

The data controller must:

- not give the DPO instructions regarding the performance of tasks
- ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
- not dismiss or penalise the DPO for performing the tasks required of them.

As a minimum a Data Protection Officer must:

- inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- provide advice on a DPIA
- co-operate with the Information Commissioner
- act as the contact point for the Information Commissioner
- monitor compliance with policies of the controller in relation to the protection of personal data
- monitor compliance by the controller with data protection law.

An independent school may also wish to appoint a Data Manager or Information Governance Lead. Schools are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- oversee the System Controllers.

Senior school leaders are responsible for the various types of data being held (e.g. learner information / staff information / assessment data etc.). These staff members will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time, and
- who has access to the data and why.

Everyone in the school has the responsibility of handling protected or sensitive data (including learner data) in a safe and secure manner.

Governors/proprietors of independent schools are required to comply fully with this policy where they have access to personal data as part of their role (either in the school or elsewhere if on school business).

Training & awareness

All staff should receive data handling awareness / data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff/NQTs
- Regular data protection/online safety training for all staff
- Day to day support and guidance

Freedom of Information Act

All local authorities must have a Freedom of Information Policy which sets out how it will deal with FOI requests. FOI aims to increase "openness by design" in public sector organisations as part of a healthy democratic process. FOI requests are submitted by an individual and the local authority is required to consider whether the requested information should be released into the public domain. Any requests for personal data should be dealt with under data protection law. The FOI Section 40(1) and (2) exemption covers personal data.

Cloud Hosting Services

Schools that use cloud hosting services should assess the risk of sharing personal data with any other third party and should identify the correct lawful basis for this data sharing. It is likely that parent/carer consent may be required in order to create an account.

C3 Mobile Technologies Policy Template (inc. BYOD/BYOT)

This guidance is for use by schools where local authority guidance/policy is not mandated.

Local authority schools should use their local authority guidance/policy as stipulated.

Mobile technology devices may be a school/local authority owned/provided or privately owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school/local authority wireless network.

The absolute key to considering the use of mobile technologies is that the learners, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the safeguarding policy, anti-bullying policy, acceptable use policy, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies that should be embedded within online safety policy and guidance. These include; security risks in allowing connections to your school/local authority network, filtering of personal devices, breakages and insurance, access to devices for all learners, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership.

Independent schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

Schools should be aware that learners who are allowed to bring their own devices to school can access mobile data through their normal data plan and the school should ensure that expectations about appropriate online behaviours are part of online safety policy and acceptable use agreements.

A range of mobile technology implementations is possible. The school should consider the following statements and remove those that do not apply to their planned implementation approach.

- The school acceptable use agreements for staff, learners and parents/carers will give consideration to the use of mobile technologies
- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

	School/devices			Personal devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[3]	Learner owned	Staff owned	Visitor owned
Allowed in the school	**Yes**	**Yes**	**Yes**	Yes/No[4]	Yes/No[4]	Yes/No[4]
Full network access	*Yes*	*Yes*	*Yes*			
Internet only						
No network access						

- The school/local authority has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete/amend as appropriate):
- All school/local authority devices are controlled though the use of a Mobile Device Management (MDM) solution

[3] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school

[4] The school should add below any specific requirements about the use of personal devices in the school e.g. storing in a secure location, use during the day, liability, taking images etc

- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
- The school/local authority has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link between an MDM solution and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
- *All devices are subject to routine monitoring*
- *Pro-active monitoring has been implemented to monitor activity*
- *Where personal devices are permitted:*
    - *All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access*
    - *Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school*
    - *The school/local authority accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)*
    - *The school/local authority accepts no responsibility for any malfunction of a device due to changes made to the device while on the school/local authority network or whilst resolving any connectivity issues*
    - *The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security*
    - *The school/local authority is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues*

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements. In addition:

- Users are responsible for charging devices and for protecting and looking after their devices while in the school

- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use
- Images may only be taken in line with the school/local authority's digital and video images policy
- Approved devices may be used in formal exams in accordance with local authority/school policy
- Visitors should be provided with information about how and when they are permitted to use mobile devices in line with local safeguarding arrangements and policy
- *Devices may be used in lessons in accordance with teacher/school direction*

School/local authority devices

- School devices are provided to support learning. It is expected that learners will bring devices to the school as required.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc...) that would stop the device working as it was originally set up and intended to work is not permitted
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to learners on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.

Personal

- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day
- *Staff owned devices should only be used for personal purposes during school hours within the agreed school policy*
- *Printing from personal devices will not be possible*

Insurance

Schools that have implemented an authorised device approach (1:1 deployment) may wish to consider how they will insure these devices and should include details of the claims process in this policy.

C4 Social Media Policy Template

Social media (e.g. Facebook, Twitter, LinkedIn, Instagram etc) is a broad term for any kind of online platform which enables people to directly interact with each other. However, websites, some games, for example Minecraft or World of Warcraft and video sharing platforms such as YouTube and TikTok have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and learners are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Scope

This policy is subject to the school codes of conduct and acceptable use agreements.

This policy:

- applies to all staff and to all online communications which directly or indirectly, represent the school
- applies to such online communications posted at any time and from anywhere
- encourages the safe and responsible use of social media through training and education
- *defines the monitoring of public social media activity pertaining to the school.*

The school respects privacy and understands that staff and learners may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with learners are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- SLT
    - Facilitating training and guidance on Social Media use.
    - Developing and implementing the Social Media policy.
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
    - Receive completed applications for social media accounts.
    - Approve account creation.

- Administrator/moderator
    - Create the account following SLT approval.
    - Store account details, including passwords securely.
    - Be involved in monitoring and contributing to the account.
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring).

- Staff
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies.
    - Attending appropriate training.
    - Regularly monitoring, updating and managing content they have posted via school accounts
    - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone

wishing to create such an account must present a business case to the Leadership Team which covers the following points:-

- the aim of the account
- the intended audience
- how the account will be promoted
- who will run the account (at least two staff members should be named)
- will the account be open or private/closed
- how the account will be secured (e.g. strong password and 2-step verification)

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents/carers.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely serious by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.

- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive or inappropriate use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media and communications technologies does not infringe any legislation or breach confidentiality.

Handling abuse

- When acting on behalf of the school, respond to harmful or offensive content swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through online communications, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when publishing online content may include:

- engaging
- conversational
- informative
- professional

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload learner pictures online other than via official school channels.
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Learners should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- Staff
    - Personal communications are those made via personal online accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
    - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
    - Where excessive or inappropriate personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
    - The school permits reasonable and appropriate access to private social media sites.

- Pupil/Learners
    - Staff are not permitted to follow or engage with current or prior learners of the school on any personal online account. *(The school may wish to define a time period re prior learners)*
    - The school's education programme should enable the learners to be safe and responsible users of social media.
    - Learners are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

- Parents/Carers
    - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
    - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
    - Parents/carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private.
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts.
- Check your settings regularly and test your privacy.
- Keep an eye on your digital footprint.
- Keep your personal information private.
- Regularly review your connections/'friends' – keep them to those you want to be connected to.
- When posting online consider; scale, audience and permanency of what you post.
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school.
- Use a disclaimer when expressing personal views.
- Make it clear who is posting content.

- Use an appropriate and professional tone.
- Be respectful to all parties.
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author.
- Express opinions but do so in a balanced and measured manner.
- Think before responding to comments and, when in doubt, get a second opinion.
- Seek advice and report any mistakes using the school's reporting process.
- Consider turning off tagging people in images where possible.
- Ensure the account is set up securely and the account can be transferred to another approved staff member in the event of the account holder leaving the school.

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute.
- Don't publish confidential or commercially sensitive material.
- Don't breach copyright, data protection or other relevant legislation.
- Don't link to, embed or add potentially inappropriate content. Consider the appropriateness of content for any audience of school accounts.
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content.
- Don't use social media to air internal grievances.

Links to other organisations or documents

The following links may help those who are developing or reviewing a school Online Safety Policy and creating their online safety provision:

Scottish Government

- ICT in Education
- Glow
- Better relationships, better learning, better behaviour (to be updated late 2017)
- National Action Plan on Internet Safety for Children and Young People
- A National Approach to Anti-bullying for Scotland's Children and Young People http://www.gov.scot/Publications/2010/11/12120420/0 (to be updated late 2017)
- Guidance on Developing Policies to Promote the Safe and Responsible Use of Mobile Technology in Schools - http://www.gov.scot/resource/0043/00438214.pdf

UK Safer Internet Centre

UK Safer Internet Centre

South West Grid for Learning

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

Report Harmful Content

UK Safer Internet Centre – Research Summaries

Others

CEOP / ThinkUKnow

INSAFE/Better Internet for Kids

UK Council for Internet Safety (UKCIS)

NCA – CyberChoices

Tools for Schools

SWGfL Test filtering

UKCIS Digital Resilience Framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Scottish Anti-Bullying Service, respect*me* - http://www.respectme.org.uk/

Scottish Government - Better relationships, better learning, better behaviour

Childnet – Project deSHAME – Online Sexual Harassment

Data Protection

Scottish Government / Scottish Information Commissioners Office:

Biometric recognition technology in schools advice note

Its public knowledge (guidance for public authorities on FOI)

Information Commissioners Office –

ICO Scotland

ICO Guidance on taking photos in schools

IRMS Information Management Toolkit for Schools

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring

NCA Guide to the Computer Misuse Act

NEN Advice and Guidance Notes

SWGfL – Test Filtering

Working with parents and carers

Education Scotland's parentzone https://education.gov.scot/parentzone/

ParentClub.scot

UKSIC pages for parents

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Internet Matters

Prevent

Prevent Duty Guidance – Scotland

Prevent for schools – teaching resources

Research

Ofcom –Making sense of media

C5 Summary of Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990

The Computer Misuse Act 1990 sets out the offences associated with computer misuse. This Act makes specific unauthorised acts or access to computer material unlawful.

Data Protection Act 2018

This Act sets out the framework for data protection law in the UK and supplements the UK General Data Protection Regulations (GDPR). The UK GDPR sets out the key principles, rights, and obligations for the processing of personal data in the UK. The term "processing" includes (but is not limited to) the obtaining, recording, holding, using, organising, disclosing, altering, or erasing of personal data. The UK GDPR sets out seven key data protection principles that are to be complied with when processing personal data. These principles require data to be:

- lawfully, fairly and transparently processed
- processed only for the purposes for which it is obtained
- adequate, relevant and limited to what is necessary
- accurate and not misleading as to any matter of fact
- kept no longer than necessary
- kept secure to prevent unauthorised or unlawful use
- taken responsibility for

Additionally, personal data must be processed in accordance with data subjects' rights and must not be transferred to other countries that do not have the same level of data protection.

Freedom of Information (Scotland) Act 2002

This Act gives individuals the right to request information held by public authorities listed in schedule 1 of that Act. Such public authorities, and companies wholly owned by public authorities, have obligations under the Act and are to follow a number of set procedures when responding to requests.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment- or a fine. This wording is important because an offence is complete as soon as a grossly offensive, indecent, obscene or menacing message has been sent: there is no need in relation to that offence to prove any intent or purpose.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

The law of copyright is governed by the Copyright, Designs and Patents Act 1988 and an automatic copyright arises when an original piece of work (for example, artistic, dramatic, literary or musical works) is created.

Copyright essentially provides the copyright owner with exclusive rights to copy their work and issue copies or communicate their work to the public. If a third party does so, without the author's permission, this is likely to be copyright infringement.

Criminal Justice and Licensing (Scotland) Act 2010

This establishes that it is an offence for a person: to behave in a threatening or abusive manner where that behaviour would be likely to cause a reasonable person to suffer fear or alarm and he or she either intends by the behaviour to cause fear or alarm or is reckless as to whether the behaviour would cause fear or alarm. This applies to behaviour of any kind, including things said or otherwise communicated as well as things done, and that it applies both in respect of behaviour consisting of a single act and behaviour consisting of a course of conduct (e.g. the repeated sending of threatening texts or emails or repeatedly following them from their home or place of work).

Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005

This legislation introduced a new offence of sexual grooming of a person under 16; It introduces a new offence of paying for the sexual services of a person under 18; It introduces new offences of causing, inciting, controlling, arranging or facilitating the provision of sexual services by children or child pornography; It amends current legislation criminalising the taking, possessing and distribution of indecent images of children so that it applies to images of people under 18 rather than only to images of those under 16.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. It also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Civic Government (Scotland) Act 1982

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- the right to a fair trial
- the right to respect for private and family life, home and correspondence
- freedom of thought, conscience and religion
- freedom of expression
- freedom of assembly
- prohibition of discrimination
- peaceful enjoyment of possessions
- the right to education
- the right not to be subjected to inhuman or degrading treatment or punishment

The school is obliged to respect these rights and freedoms, but should balance them against those rights, duties and obligations, which arise from other relevant legislation.

Children and Young People (Scotland) Act 2014

This Act requires Scottish Ministers and public authorities to consider steps which could be taken to secure better or further effect in Scotland of the United Nations Convention on the Rights of the Child (UNCRC) requirements and to prepare reports on what steps have been taken.

UNCRC requirements include prioritising the best interests of the child, respect for the views of the child, freedom of expression, freedom of thought, belief and religion, freedom of association, right to privacy, right to access information from the media, right to education, protection from sexual and other exploitation etc.

Education Scotland Act 1980

This Act requires education authorities to secure adequate and efficient provision of school and further education in their area. The Act also provides means for Scottish Ministers to intervene in certain circumstances where an independent school is objectionable or at risk of becoming so, or where a responsible body has failed to discharge a statutory educational duty etc.

Standards in Scotland's Schools etc. Act 2000

This Act enshrines children's rights to school education and to have their views taken into account in decisions that affect them. It further requires Scottish Ministers and education authorities to have regard to the need to reduce inequalities of outcomes – whether arising out of socio-economic disadvantage or otherwise – when exercising their functions relating to school education.

Scottish Schools Parental Involvement Act 2006

This Act make further provision for the involvement of parents in their children's education (and in school education generally) and provides for the establishment of Parent Councils.

Equality Act 2010

This Act prohibits discrimination, harassment and victimisation (in certain circumstances) against people who possess one of the following protected characteristics: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex, and sexual orientation.

Online Safety Act 2023

The Online Safety Act enhances the safety of users on the internet, particularly focusing on the protection of children and vulnerable individuals from harmful online content. The Online Safety Act defines 'priority offences' including

- child sexual abuse and grooming;
- encouraging or assisting suicide or serious self-harm;
- harassment, stalking, threats and abuse;
- controlling or coercive behaviour;
- intimate image abuse;
- sexual exploitation of adults

It focusses on online services which host content posted by other people ("user-to-user services" such as Facebook, Instagram and Twitter) and search services (such as Google, Yahoo and Bing). The Bill has different levels of protection for children and adults.

Protections for young people

The Online Safety Act creates a legal responsibility (a "duty of care") for the operators of user-to-user services to protect users under the age of 18 from harmful content, specifically

- Enforcing minimum age requirements
- Publishing risk assessments
- Protecting children from harmful content published on the service
- Properly applying the Terms and Conditions

Protections for adults

While the Bill focusses on the need to protect young people online, there are some provisions that focus on protecting adults (which will benefit all users) including

- Ability to customise your feed
- Block online trolls
- Criminalising certain content
- Remove content that is already illegal

Enforcement

Ofcom has been appointed as the regulator and have powers to obtain information from website operators on how they deal with online harms and to take action if they fail to comply with their new duties, including

- Investigate website operators and their compliance with the Bill
- Issue financial penalties to companies that do not comply with their obligations
- Issue guidance on compliance
- Issue notices requiring website operators to give information or cooperate with an Ofcom investigation