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, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Any illegal activity for example: • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • 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..					X
Users shall not undertake activities that might be classed as cyber-crime under the	• 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					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
computer Misuse Act (1990)	• 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 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	

Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.	Staff and other adults				Learners			
	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.

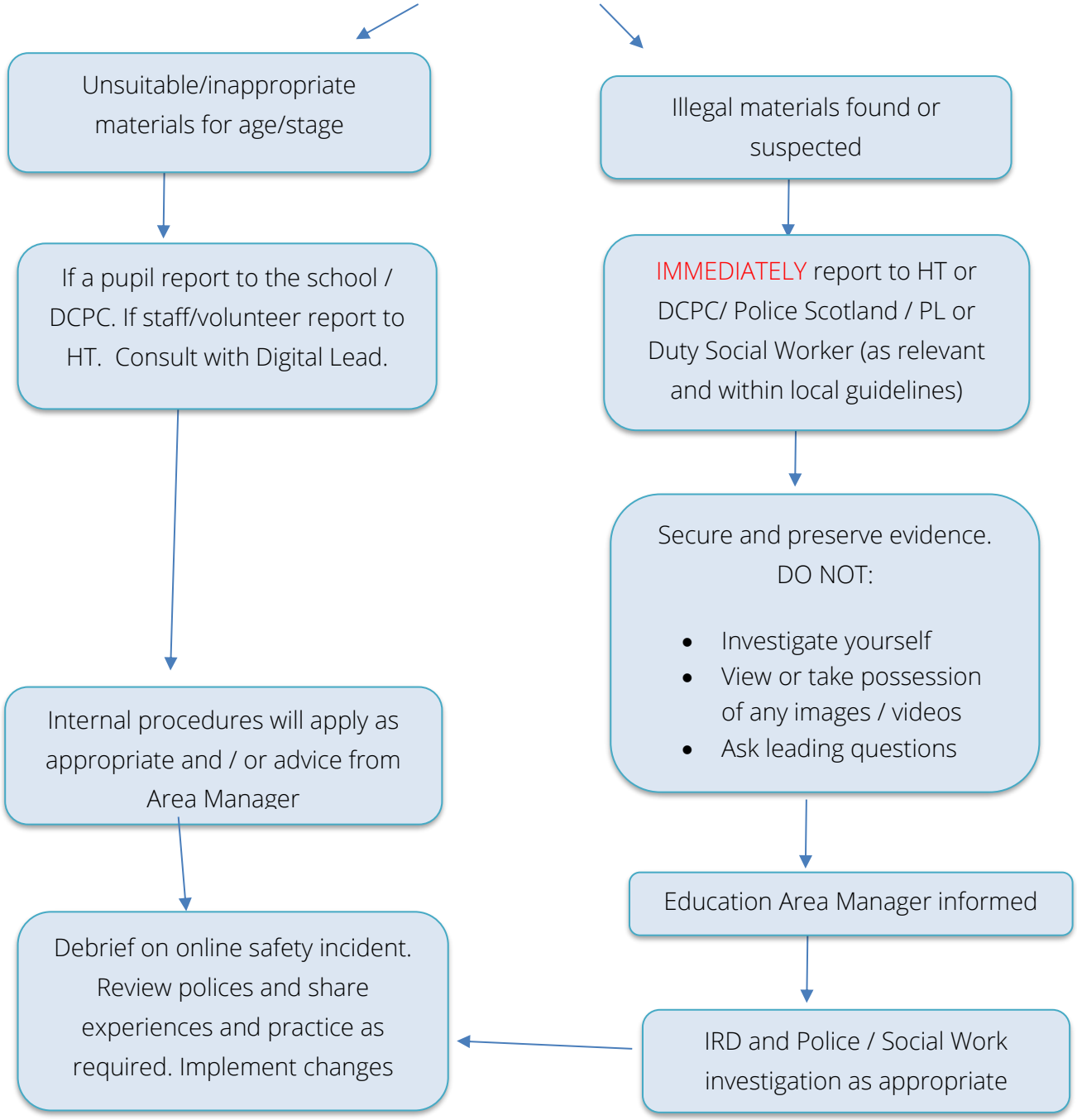
(Schools may wish to consider the use of online/anonymous reporting systems, which can be used by all members of the school community)

- 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

[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.

Full network access (e.g. file systems)					
Internet only					
No network or internet access					

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 risks, 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:

person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in May 2022. However, SWGfL cannot guarantee it's accuracy, nor can it accept liability in respect of the use of the material.