Glenbervie School

Online Safety Policy

Including Social Media Policy

Updated March 2025

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: 1 (revised)

Date created: [06/03/25]

Next review date: [06/03/26]

Scottish Government
Riaghaltas na h-Alba
gov.scot

Contents

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Glenbervie School 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).

Glenbervie School 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 Digital Leaders made up of:

- *Mrs Karen Johnstone - Headteacher/ child protection/safeguarding lead*
- *Mrs Lisa McConachie - Online Safety Lead*
- *Staff – including teachers/support staff*
- *Parents and carers*
- *Digital Leaders*

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:	*March 2018*
The implementation of this Online Safety Policy will be monitored by:	Mrs Johnstone and the Glenbervie Digital Leaders
Monitoring will take place at regular intervals:	*Termly*
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:	*Twice Annually – November and March*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Paul Rooke - QIO* *Aberdeenshire Council Love Learning Team* *Laura Anderson – Stonehaven Social Work* *Mark Bolton – Youth Engagement Officer, Police*

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *monitoring logs of internet activity (including sites visited)*
- *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 : Karen Johnstone

- 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 Online Safety Lead 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 is 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 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.

Online Safety Lead: Lisa McConachie

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 head teacher/child protection/safeguarding lead
- 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.

Teaching and support staff

School staff are responsible for ensuring that:

Curriculum Leads will work with the online safety lead to develop a planned and coordinated online safety education programme. This will be provided through:

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

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 *head teacher* 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
- 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
- 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*

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.

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 has the following members:

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

Members of the Digital leaders Group will assist the Online Safety Lead 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 including In-Service activity and shared in our staff SharePoint site.
- 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. At Glenbervie we issue a Microsoft Form for Parents to confirm they have read through the AUP, with their children, and understand their roles and responsibilities.

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 around the school. *Glenbervie Digital Leaders 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:

- Policy Documents available in staffroom
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- peer supp

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,	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					**X**

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
remarks, proposals or comments that contain or relate to:	• Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering 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) 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					**x**

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	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 teaching staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online Gaming	X				X			
Online shopping/commerce			X		X			

File sharing (sharing files with HT or teacher).		X						X
Social media			X		X			
Messaging/chat			X		X			
Entertainment streaming e.g. Netflix, Disney+			X		X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok			X		X			
Mobile phones may be brought to school		X					X	
Use of mobile phones for learning at school		X			X			
Use of mobile phones in social time at school		X			X			
Taking photos on mobile phones/cameras			X		X			
Use of other personal devices, e.g. tablets, gaming devices			X		X			
Use of personal e-mail in school, or on school network/guest wi-fi			X		X			
Use of school e-mail for personal e-mails	X				X			

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

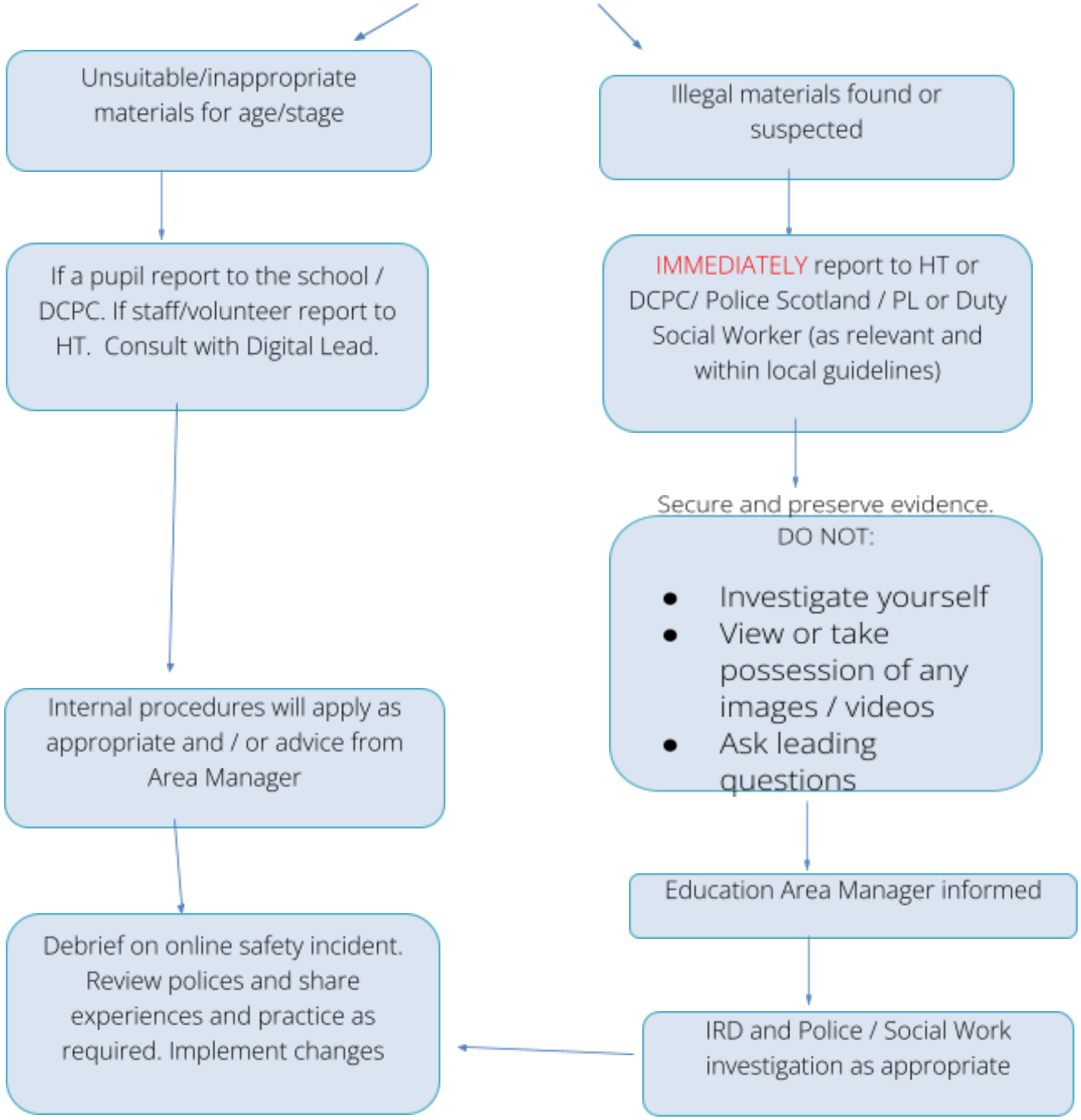
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- 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.
- 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 within the 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
- learning from the incident (or pattern of incidents) will be provided 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 following 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:

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 rights	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	X	X	X			X			
Corrupting or destroying the data of other users.	X	X	X						
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	X		
Unauthorised downloading or uploading of files or use of file sharing.	X		X						

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

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.	X	X				X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X		X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X	X		
Using proxy sites or other means to subvert the school's filtering system.		X				X		
Unauthorised downloading or uploading of files or file sharing		X			X	X		
Breaching copyright or licensing regulations.	X	X	X			X		
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.	X	X				X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X		
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers		X						

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

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.

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 using Project EVOLVE

- the programme should build on prior knowledge and experience of pupils in order to ensure relevance and interest using 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:

- *mechanisms to seek learner feedback and opinion to inform online safety policy and practice*
- *appointment of digital leaders/young leaders*
- *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*

Staff/volunteers

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

- 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
- 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

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.

Parental Engagement

Many parents and carers may 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:

- *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.*

Glenbervie 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

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

- 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
- 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, they 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.
- 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
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person
- 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 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.

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*
- *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.

Technical Security

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 and 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,
- 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

- 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
- 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 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.

The school acceptable use agreements for staff, learners, parents and carers outline the expectations around the use of mobile technologies.
The school allows:

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

School owned/provided devices:

- Inventory of devices and allocation held by Digital Leader and staff
- Devices should not be used at lunch or break times and a teacher must be present.

[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.

- Staff (and students – if asked by staff) may download apps from the self-service app managed by the LoveLearning team.
- Aberdeenshire Council wifi is restricted
- ITHub should be used to log any issues
- Aberdeenshire Council sets the filters however staff can send web addresses to Glow Admin or ITHub to be added to the filter.
- Aberdeenshire Council ITHub team provide the necessary protection for devices. Digital Leaders and teachers will regularly check for updates to ensure iPads have the latest updates installed for security purposes.
- Staff have access to corporate Microsoft OneDrive, Microsoft OneDrive and Google Drive on Glow. Pupils have access to Microsoft OneDrive and Google Drive on Glow.
- Staff data protection, Cyber Security and GDPR courses available on ALDO these must be completed.
- Should school iPads should be used to take photos, permissions must be checked prior to taking the photos. Images should be saved in OneDrive and deleted once used.
- When a user leaves the school staff accounts are closed and data delete by IT. Pupil accounts are transferred to the receiving school.
- Staff will be given regular training on software and online safety.

Personal devices

- Visitors to the school may use their devices however they are unable to access the school network or wifi.
- Staff will be able to use personal devices within class but should ensure GDPR is adhered to when completing schoolwork on a personal device.
- Wifi is available to staff on personal devices for the purpose of schoolwork both during and out of school hours.
- ITHub or the LoveLearning team should be used with any technical support that requires advanced support.
- One drive should be used to save/move data.
- When using personal devices within school and on the school network the school cannot be held responsible for loss/damage or malfunction to the device.
- Any personal devices being used within school should be clearly labelled.
- Visitors will be shown the policy and protocols prior to accessing devices.
- As part of the digital education, pupils will be taught how to stay be safe and responsible when using mobile devices.
- Mobile devices will follow the same procedures as identified with the digital devices.

Social media

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.

Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- 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 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.
- 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:

- *Public-facing website*
- *Social media – Facebook Group*
- *Groupcall, Clickview*
- *Newsletters*

The school website is managed/hosted by the Head Teacher. 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 by publishing the schools Online Safety Policy.

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

All Aberdeenshire 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
- All staff are aware of the relevant Data Protection Policy
- 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 are in place to enable staff to work from home (e.g. VPN access to the school network, or a work laptop provided).

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

The school:

- *has a Data Protection 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.*
- *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,*
- *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.
- 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:

Copyright of these policy templates is held by SWGfL. Schools and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any 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.

© SWGfL 2022

Appendices

A1 Acceptable Use Agreement – for Staff, Community Users and Volunteers
A2 Learner Acceptable Use Policy Agreement Template – for Parents Nursery to P7
A4 Parent/Carer Acceptable Use Agreement Template and permission forms
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
Links to other organisations or documents

A1 Learner Acceptable Use Agreement

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. 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
- 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.
- 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.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- 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 not use personal e-mail addresses on the school systems.
- 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 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 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: _____

ways of locating and using

th and complexity (eg three-
ls found in Glow Connect -
ct)
rself and not share them with

rd I will speak to my teacher

omputer/device.
hout their permission.

bad language.
be traced back to me.
istribute files that could be
or that harasses or insults

ome address, phone number

w or my teacher knows.
on about other people into

l to via the internet or Glow.
or other pupils without their

tographs or videos of others

r the use of text, multimedia
or blog sites is unacceptable
ences.
or pictures from the internet
I have appropriate copyright

or that upsets me in emails,
adult and/or use the Report
e screen.

- I understand that device use and activity (eg browser history) can be monitored by Aberdeenshire Council and may be subject to random spot-checks of browser history and device content and configuration.
- I understand that if I am irresponsible in my use of IT, the internet or Glow, my access in school may be removed.
- I understand that if I abuse the privilege, that staff may sometimes allow me, of using my own device or mobile phone in class, my device may be temporarily confiscated with proportionate sanctions, up to and including Police involvement.
- I understand the same sanctions will apply if I use my own device in class without permission.
- I am responsible for taking care of any personal device I bring to school.
- I understand that any device which I connect to the network should not pose a threat to the network through its contents or through downloads.

that these rules apply when my child is using IT (including both school and personal computers and devices) and the internet.

I have gone through the rules with my child and explained their importance and the consequences of breaking the rules, and ensured that they understand.

I understand that the school will make every reasonable effort to filter out access to controversial material on the Internet, but I will not hold them responsible for materials my son or daughter acquires or sees as a result of the use of IT at school.

I also accept that the school cannot be responsible for any loss, theft or damage to personal equipment my child may bring to school e.g. smartphone, iPod, netbook etc.

I understand that if a school-provided device is used at home, parents/carers are responsible for providing any content filtering or restrictions on their own networks and monitoring home usage and any intentional or negligent damage to this device may be subject to the cost of repair or replacement.

I understand that in order to provide my child with a Glow Account some information will be transferred from school to Glow.

I give my permission to allow the child/young person named above to use IT and the internet in school. *(This can be changed at any time by contacting the Head Teacher.)*

Parent's / Carer's signature and date

.....

Learner (P4 and above)

I have read the rules for Acceptable IT and internet Use and know the importance of these rules.

I know that if I break these rules, I may lose the right to use the school's computer facilities or face further disciplinary action.

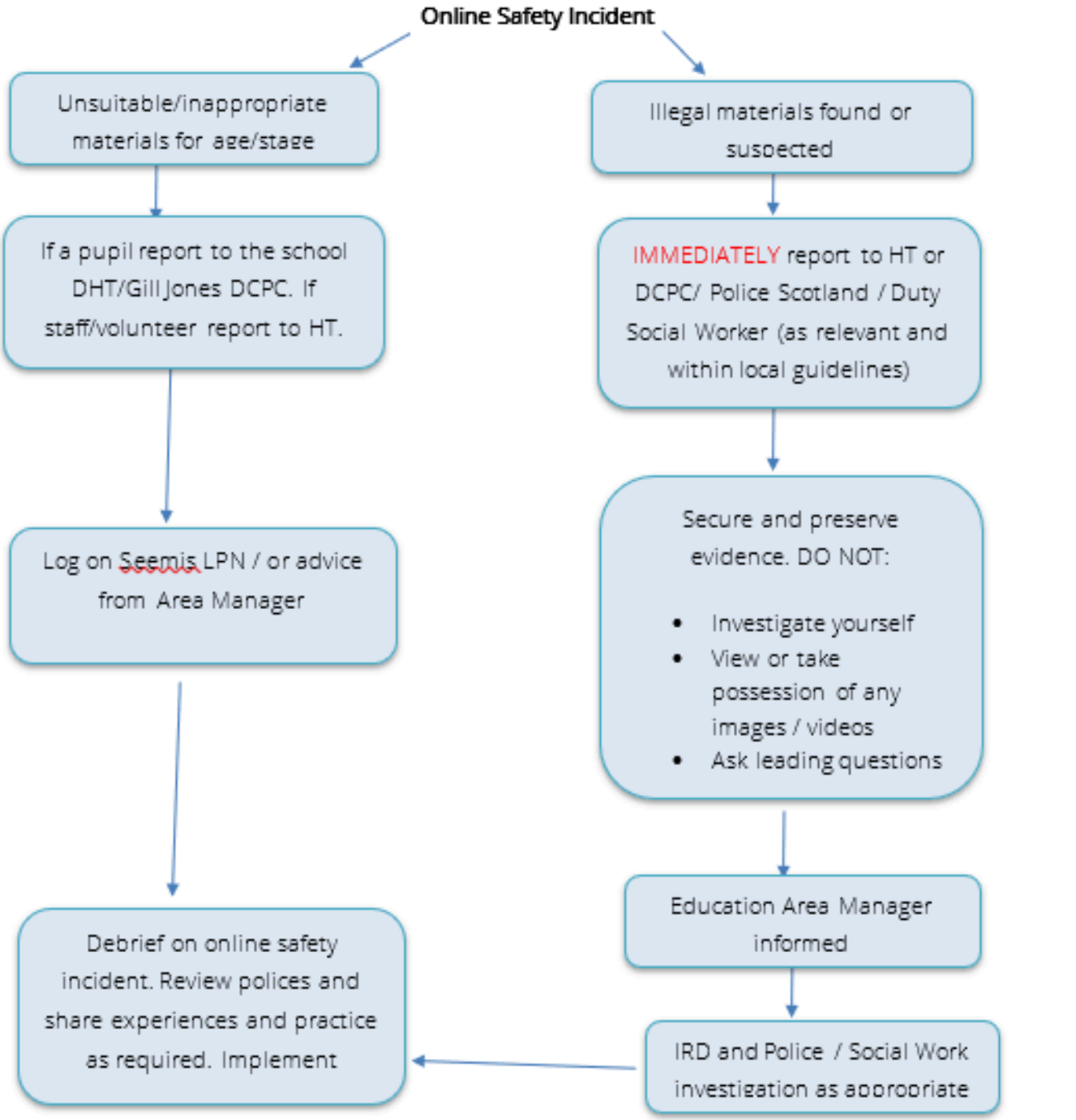
Learner's signature and date

.....

&
of IT in
hools

These rules apply to all uses of the internet and to all information sent electronically, including text messages and pictures sent by mobile phones.

A7 Responding to incidents of misuse – flow chart



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

C2 Personal Data Advice and Guidance

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. Aberdeenshire council requires school to conduct a DPIA before processing activity starts and run alongside the planning and development process.

- **Step 1:** Check Data Protection page on Arcadia for current DPIA
- **Step 2:** Identify the need for using personal data
- **Step 3:** Describe the information flows
- **Step 4:** Identify the privacy and related risks
- **Step 5:** Identify privacy solutions
- **Step 6:** Sign off and record the DPIA outcomes
- **Step 7:** 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 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 (inc. BYOD/BYOT)

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.

- The school acceptable use agreements for staff, learners and parents/carers will give consideration to the use of mobile technologies
- The school allows:

	School/devices			Personal devices		
	School owned and allocated	School owned for use by	Authorised device[2]	Learner owned	Staff owned	Visitor owned

[2] 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

	to a single user	multiple users				
Allowed in the school	**Yes**	**Yes**	**NA**	**Yes**	**Yes**	**Yes**[4]
Full network access	*Yes*	*Yes*	NA	No	No	No
Internet only	Yes	Yes	NA	Yes	Yes	Yes
No network access	Yes	Yes	NA	Yes	Yes	Yes

- The school/local authority has provided technical solutions for the safe use of mobile technology for school devices:
- All school/local authority devices are controlled though the use of a Mobile Device Management (MDM) solution
- 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 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.**
- 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
- Printing from personal devices will not be possible

C4 Social Media Policy

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.

.

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. Staff should also contact Aberdeenshire Council Communications unit for advice 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'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

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use. Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in September 2022. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.