*Glenbervie School*

**

Online Safety Policy

Including Social Media Policy

Updated March 2022

This policy applies to all members of the schoolcommunity (including staff, children / young people, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school.

## Development/Monitoring/Review of this Policy

4

This online safety policy has been developed by a working group/committee – **Digital leaders** made up of:

* Headteacher- JennyGlennie
* Online safety officer/coordinator – Lisa Mc Conachie
* Staff – including practitioners/support staff- Admin Team
* Parents and carers
* Community users

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

Schedule for Development/Monitoring/Review

5

|  |  |
| --- | --- |
| This online safety policy was agreed: | June 2017 (updated December 2018) |
| The implementation of this online safety policy will be monitored by the: | Digital Leader Group & Head Teacher |
| Monitoring will take place at regular intervals: | Annually |
| The *Headteacher* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | Twice a year- December & June |
| The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | March 23 or when required |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | **Head Teacher*,* local authority Child Protection lead officer, duty social work team, police** |

The school will monitor the impact of the policy using:

* *Logs of reported incidents*
* *Monitoring logs of internet activity (including sites visited)*
* *Internal monitoring data for network activity*

## Scope of the Policy

6

7

This policy applies to all members of the school community (including staff, children / young people, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technologies ICT systems, both in and out of the school.

* Health and Wellbeing is one of the eight curricular areas in Curriculum for Excellence. Its **substantial importance is reflected in its position at the centre of the curriculum and at the heart of children’s learning** – as well as a central focus of the Scottish Attainment Challenge and the National Improvement Framework for Education. Along with literacy and numeracy it is one of the three core areas that are the **responsibility of all staff in the school**.

* Learning in Health and Wellbeing is designed to ensure that children and young people develop the knowledge and understanding, skills, capabilities and attributes which they need for **mental, emotional, social and physical wellbeing** now and in the future.
* Health and Wellbeing is also about the **whole approach of the school**. Children and young people should feel happy, safe, respected and included in the learning environment and all staff should be proactive in promoting positive relationships and behaviour in the classroom, playground, and wider learning community.
* Health and Wellbeing is also about the whole approach of the nursery, school, college or other setting. The ethos should support what children are learning and the climate – the behaviour that’s modelled and encouraged – should reflect this.
* Schools need to be aware that incidents of online bullying, or other online safety incidents covered by this policy may take place outside of the school, between children and young people who attend the school or between any members of the school community, including staff. The school and the local authority, in partnership with parents and carers need to decide how to deal with such incidents and make this clear in the policy. This will link closely with positive relationships and behaviour policy and anti-bullying policies. The policy should make clear how the school will involve parents and carers in relation to such incidents.

## Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals[[1]](#footnote-1)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.

### Head Teacher :

* The Head Teacherhas a duty of care for ensuring the safety (including online safety) of members of the school community.
* The Head Teacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
* The Head Teacher is responsible for ensuring that the online safety co-ordinator/officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
* The Head Teacher 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. This is to provide a safety-net and also support to those colleagues who take on important monitoring roles.
* The Head Teacher will receive regular monitoring reports from the online safety co-ordinator/officer.

### Online safety co-ordinator/officer:

The online safety co-ordinator*/officer: Lisa McConachie/ Jenny Glennie (small school so shared)*

* leads the online safety group
* takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
* ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
* Ensures they are up to date with national relationships and behaviour guidance and anti-bullying guidance
* provides (or identifies sources of) training and advice for staff
* records incidents of online bullying through the school’s SEEMiS recording system in line with local procedures
* liaises with the local authority/relevant body
* liaises with (school) technical staff
* receives reports of online safety incidents and creates a log of incidents to inform future online safety developments. **The school will deal with these incidents and the investigation/action will be the responsibility of the Online safety co-ordinator and Head Teacher.**
* meets regularly with relevant officer from the Local Authority to discuss current issues, review incident logs and if possible, filtering change control logs
* reports regularly to Head Teacher

### Designated Getting it right for every child - Named Persons: Jenny Glennie

Getting it right for every child is the national approach in Scotland that puts the rights and wellbeing of children and young people at the heart of services that support them and provides a framework within which services can offer the right help, at the right time, from the right people.

The Getting it right for every child approach includes making available a Named Person for every child, from birth, until they reach 18, or beyond if they are still in school.

The approach builds on good practice by making a clear point of contact available for all children and young people, usually via the Health Visitor or a promoted teacher for children in school. In schools, the role of Named Person will be taken forward by these individuals as an integrated part of their existing duties: offering advice or support relevant to their expertise, or helping access support from others. It is national policy for local authorities to make the Named Person service available as an entitlement, but there is no obligation for children and young people or parents to accept any offer of advice or support from the Named Person.

### Network manager/technical staff: Aberdeenshire council

Thenetwork manager/technical staff(or managed service provider) is responsible for ensuring:

* **that the school technical infrastructure is secure and is not open to misuse or malicious attack**
* **that the schoolmeets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body and also the online safety policy / guidance that may apply**
* **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
* **that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as appropriate.**
* **that the use of the network / internet / learning platform / VLE / remote access / email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head Teacher**

### Teaching and Support Staff

Are responsible for ensuring that:

* **they have an up to date awareness of online safety matters and of the current schoolonline safety policy and practices**
* **they have read, understood and signed the staff acceptable use policy (AUP)**
* **they report any suspected misuse or problem to the Head Teacher forinvestigation / action**
* **all digital communications with children / young people/parents and 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 using the refreshed curriculum guidance in the Technologies experiences and outcomes.
* children / young people understand and follow the online safety and acceptable use policies
* children / young people have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* they 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

### Child Protection Coordinator ; Jenny Glennie

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

* sharing of personal data[[2]](#footnote-2)
* access to illegal/inappropriate materials
* inappropriate online contact with adults/strangers
* potential or actual incidents of grooming

### Online safety group- Digital Leaders

The online safety group[[3]](#footnote-3) provides a consultative group that has wide representation from the schoolcommunity, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to senior management.

Members of the online safety group will assist the online safety co-ordinator/officer (or other relevant person, as above) with:

* the production / review / monitoring of the school online safety policy / documents in line with local anti-bullying policies.
* mapping andreviewing the online safety curricular provision – ensuring relevance, breadth and progression using the refreshed curriculum guidance in the Technologies experiences and outcomes.
* monitoring network / internet / incident logs where possible
* consulting stakeholders – including parents / carers and the children / young people about the online safety provision
* monitoring improvement actions identified through use of the 360 degree safe Scotland self-review tool

### Children / young people:

* **are responsible for using the school digital technology systems in accordance with the acceptable use policy**
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* need to understand the importance of reporting online bullying incidents, abuse, misuse or access to inappropriate materials and know how to do so
* Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online bullying.
* should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school’sonline 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 internet / mobile devices in an appropriate way, protect their privacy and keep themselves safe. The school will take every opportunity to help parents understand these issues through parents’ evenings, newsletters, emails, letters, website, learning platform and information about national / local online safety campaigns / literature*.* Parents and carers will be encouraged to support the school in promoting good online safety practice, to act as good role models and to follow guidelines on the appropriate use of:

* digital and video images taken at school events
* access to parents’ sections of the website, Seesaw learning platform and online learner records
* their children’s personal devices in the school (where this is allowed)

### Community Users

Community users who access school systems / website / learning platform as part of the wider school provision will be expected to sign a community user AUP before being provided with access to school systems.

## Policy Statements

11

### Education – children / young people

Whilst regulation and technical solutions are very important, their use must be balanced by educating children / young people to take a responsible approach. The education of children / young people in online safety is therefore an essential part of the school’s online safety provision. They need the help and support of the school to recognise and avoid online safety risks and build their resilience and know who they can speak to when things go wrong.

Under Curriculum for Excellence, all adults who work in schools have a responsibility to support and develop mental, emotional, social and physical wellbeing. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across all subject areas. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: (Note: statements will need to be adapted, depending on school structure and the age of the children / young people)

* **A planned online safety curriculum as part of year group assemblies and across a range of subjects, (e.g. Computing / Personal and Social Education other lessons) should be regularly revisited (gooseberry planet)**
* **Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities. The emphasis in such messages should be on children and young people learning to protect themselves and respect others. As appropriate the planned programme should help children / young people understand what Digital Citizenship means and how it relates to the roles and responsibilities outlined in the school’s positive behaviour policy**
* **Children / young people 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.**
* **Children / young people should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
* Children / young people 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. *Nb. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.*
* Children / young people should be helped to understand the need for the learner acceptable use policy 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 internet use is pre-planned, it is best practice that children / young people 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 children / young people are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit*.*
* It is accepted that from time to time, for good educational reasons, children / young people may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other nominated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

### Education – parents and carers

Some 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 therefore seek to provide information and awareness to parents and carers through:

* Curriculum activities and Gooseberry Planet
* Letters, newsletters, website, emails, learning platform- Seesaw
* Parents and carers evenings / sessions
* High profile events/campaigns for example Safer Internet Day
* Reference to the relevant web sites / publications, e.g. [www.saferinternet.org.uk/](https://www.saferinternet.org.uk/advice-centre/social-media-guides) [http://www.childnet.com/parents-and-carers](http://www.respectme.org.uk/) (see appendix for further links/resources)

### Education – the wider community

The school may provide opportunities for local community groups / members of the 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, digital literacy and online safety
* Online safety messages targeted towards grandparents and other relatives as well as parents.
* The school learning platform, website will provide online safety information for the wider community
* Supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision (possibly supporting the group in the use of Online Compass, an online safety self review tool *-* [www.onlinecompass.org.uk](http://360safe.org.uk/Files/Documents/facebook-6))

### Education and training – staff/volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

* **A planned programme of formal online safety 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.** It is expected that some staff will identify online safety as a training need.
* **All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use policys.**
* The online safety co-ordinator / will receive regular updates through attendance at external training events, / local authority/ other relevant organisations) and by reviewing guidance documents released by relevant organisations*.*
* This online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
* The online safety co-ordinator / officer (or other nominated person) will provide advice / guidance / training to individuals as required.

### Technical – infrastructure/equipment, filtering and monitoring

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 must be securely located and physical access restricted**
* **All users will have clearly defined access rights to school technical systems and devices.**
* **All users, when deemed old enough / mature enough will be provided with a username and secure password** by admin support- through the authority who will keep an up to date record of users and their username*s.* Users are responsible for the security of their username and password.
* **The “master/administrator” passwords for the school digital systems, used by the network manager (or other person) must also be available to the Head Teacher and kept in a secure place, (e.g. school safe)**
* The school **is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations** (
* **Internet access is filtered for all users.** There is a clear process in place to deal with requests for filtering changes.
* **Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet**.
* *Where possible the local authority technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use policy*
* An appropriate system is in place (Log book via Digital Leader group) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
* Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
* An agreed policy is in place (temporary Log in passwords) 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 (authority policy) regarding the extent of personal use that users (staff/children / young people/community users) and their family members are allowed on school devices that may be used out of school.
* An agreed policy is in place (authority policy) that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
* An agreed policy is in place (authority Policy) regarding the use of removable media (eg 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 owned/provided or personally owned and might include: smartphone, tablet, 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 email 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.

* The school or local authority acceptable use policies for staff, children / young people, parents and carers will give consideration to the use of mobile technologies
* The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | School Devices | | | Personal Devices | | |
|  | School owned for individual use | School owned for multiple users | Authorised device[[4]](#footnote-4) | Owned by children / young people | Staff owned | Visitor owned |
| Allowed in school | Yes | Yes |  | No[[5]](#footnote-5) | Yes | Yes/ |
| Full network access | Yes | Yes |  |  | No | No |
| Internet only |  |  |  |  | Yes | Yes |
| No network access |  |  |  |  |  |  |

Aspects that the school may wish to consider and be included in their online safety policy, mobile technologies policy or acceptable use policies:

### Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children / young people instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and children / young people need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. 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 children / young people 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, eg., on social networking sites.**
* **Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.**
* 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 children / young people in the digital / video images.
* Care should be taken when taking digital/video images that children / young people are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
* Children / young people must not take, use, share, publish or distribute images of others without their permission
* Photographs published on the website, or elsewhere that include children / young people will be selected carefully and will comply with good practice guidance on the use of such images.
* The full names of children / young people 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 children / young people are published on the school website covered as part of the AUA signed by parents or carers at the start of the year
* The work of children / young people can only be published with the permission of the learner and parents or carers.

### Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection laws in force at the time this document is signed. Until May 2018 this will be the Data Protection Act 1998 which states that personal data must be:

* Fairly and lawfully processed
* Processed for limited purposes
* Adequate, relevant and not excessive
* Accurate
* Kept no longer than is necessary
* Processed in accordance with the data subject’s rights
* Secure
* Only transferred to others with adequate protection.

From May 2018 new regulations came into force (General Data Protection Regulations – GDPR). The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas listed in this document is ensured by Aberdeenshire Council and the school.

The school must ensure that:

* **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
* **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
* **All personal data will be fairly obtained in accordance with the privacy notice and lawfully processed in accordance with the conditions for processing.**
* **Correct permissions (from parents / carers and children / young people) are gained for use of data as relevant under current legislation**
* **It is aware of who the Data Controller within the Local Authority is**
* It has clear and understood arrangements for the security, storage and transfer of personal data
* Data subjects have rights of access and there are clear procedures for this to be obtained
* There are clear and understood policies and routines for the deletion and disposal of data
* There is a system for reporting, logging, managing and recovering from information risk incidents
* There are clear data protection clauses in all contracts where personal data may be passed to third parties
* There is clear information and advice about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office.

**Staff must ensure that they**:

* **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
* **Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.**
* **Transfer data using encryption and secure password protected devices.**

When personal data is stored on any portable computer system, memory stick or any other removable media:

* the data must be encrypted and password protected
* the device must be password protected
* the device must offer approved virus and malware checking software

16

* the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

### Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages: The school have an Acceptable Use Policy (APU) for pupils, staff and parents.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Staff & other adults | | | Children / young people | | | | | |
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to the school | x√ |  |  |  | |  |  |  |  |
| Use of mobile phones in lessons |  |  |  |  | |  |  |  |  |
| Use of mobile phones in social time |  |  |  |  | |  |  |  |  |
| Taking photos on mobile phones / cameras |  |  |  |  | |  |  |  |  |
| Use of other mobile devices e.g. tablets, gaming devices |  |  |  |  | |  |  |  |  |
| Use of personal email addresses in school, or on school network |  |  |  |  | |  |  |  |  |
| Use of school email for personal emails |  |  |  |  | |  |  |  |  |
| Use of messaging apps |  |  |  |  | |  |  |  |  |
| Use of social media |  |  |  |  | |  |  |  |  |
| Use of blogs/ Seesaw |  |  |  |  | |  |  |  |  |

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

* **The official school/local authority email service may be regarded as safe and secure and is monitored.Users should be aware that email communications are monitored.** Staff and children / young people should therefore use only the school email service 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 children / young people or parents/carers (email, chat, learning platform, etc.) must be professional in tone and content.** These communications may only take place on official (monitored) school systems.
* Young people will be provided with individual school email addresses for educational use*.*
* Children / young people 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 the need to communicate appropriately when using digital technologies.

### Social media

With an increase in use of all types of social media for professional and personal purposes our APU sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of children / young people, the school and the individual when publishing any material online. Expectations for teachers’ professional conduct are set out in the Code of Professional Conduct and the Standards for Registration (GTCS) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff.

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

* Ensuring that personal information is not published
* Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues
* Clear reporting guidance, including responsibilities, procedures and sanctions
* Risk assessment, including legal risk

School staff should ensure that:

* No reference should be made in social media to children / young people, parents and 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
* Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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, including
* 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 a 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

### Monitoring of Public Social Media

* 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

School use of social media for professional purposes will be checked regularly by a nominated senior leader and online safety group to ensure compliance with the social media, data protection, communications, digital image and video policies.

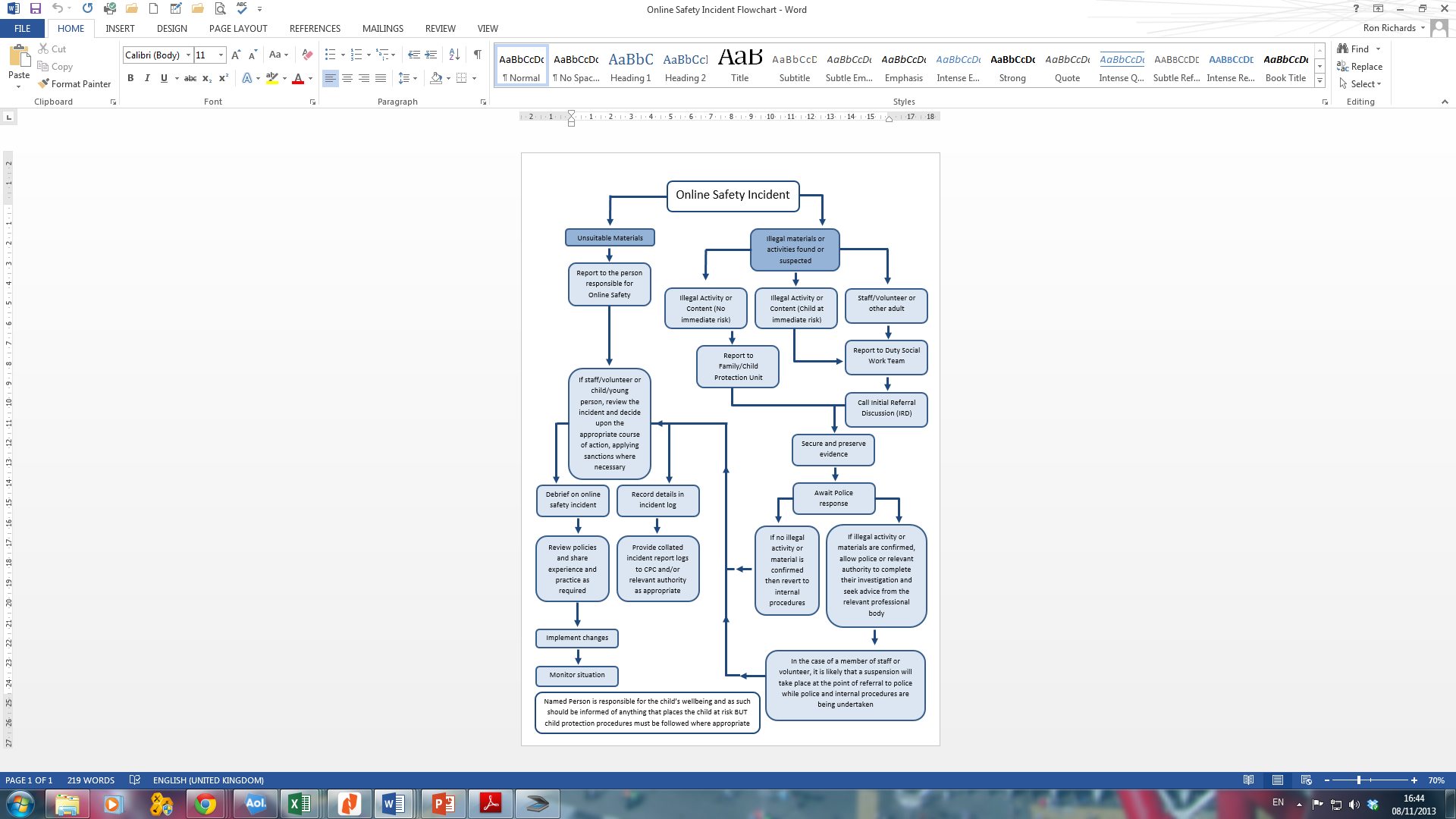
The social media policy and APU provides more detailed guidance on the school’s responsibilities and on good practice.

## Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities .

### Illegal Incidents

**If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.**



### Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, through deliberate misuse.

**In the event of suspicion, all steps in this procedure should be followed:**

* Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
* Conduct the procedure using a designated computer that will not be used by children / young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
* It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
* Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
* Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
* Internal response or discipline procedures
* Involvement by local authority or national/local organisation (as relevant).
* Police involvement and/or action
* **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police 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
* **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

### 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 agreed 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:

## Children / Young People Actions

|  |
| --- |
|  |
| children / young people incidents | Refer to class teacher | | | Refer to Headteacher | | Refer to Police | | Refer to technical support staff for action re filtering / security etc. | | Inform parents / carers | | Removal of network / internet access rights | | Warning | | Further sanction eg exclusion |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). |  | | | X | |  | | X | | X | | X | |  | |  |
| Unauthorised use of non-educational sites during lessons | X | | |  | |  | |  | |  | |  | |  | |  |
| Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device | X | | | X | |  | |  | |  | |  | |  | |  |
| Unauthorised / inappropriate use of social media / messaging apps / personal email | X | | | X | |  | |  | | X | |  | | X | |  |
| Unauthorised downloading or uploading of files | X | | | X | |  | | X | |  | | X | |  | |  |
| Allowing others to access school network by sharing username and passwords | X | | | X | |  | |  | |  | |  | |  | |  |
| Attempting to access or accessing the school network, using another child’s / young person’s account | X | | |  | |  | |  | |  | |  | |  | |  |
| Attempting to access or accessing the school network, using the account of a member of staff | X | | | X | |  | |  | |  | |  | |  | |  |
| Corrupting or destroying the data of other users | X | | | X | |  | |  | | X | |  | | X | |  |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature |  | | | X | |  | |  | | X | | X | | X | |  |
| Continued infringements of the above, following previous warnings or sanctions |  | | | X | |  | |  | | X | | X | |  | | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | | | X | |  | | X | | X | | 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 | |  |
| Deliberately accessing or trying to access offensive or pornographic material | X | | | X | | X | | X | | X | | X | |  | | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act  21 | X | | | X | |  | | X | |  | |  | |  | |  |
|  | | | |
| Staff Incidents | | | Refer to Local Authority / HR | | | Refer to Police | | Refer to Technical Support Staff for action re filtering etc. | | 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 | |
| Inappropriate personal use of the internet / social media / personal email | | |  | | |  | | X | | X | |  | |  | |
| Unauthorised downloading or uploading of files | | |  | | |  | | 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 | |  | |  | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | | |  | | |  | |  | | X | |  | |  | |
| Deliberate actions to breach data protection or network security rules | | | X | | |  | | X | |  | |  | | X | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | | X | | | X | |  | |  | |  | | X | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | | X | | |  | |  | | X | |  | |  | |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with children / young people | | |  | | |  | |  | | X | |  | |  | |
| Actions which could compromise the staff member’s professional standing | | |  | | |  | |  | | X | |  | | X | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | | X | | |  | |  | | 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 | |  | |  | |
| Deliberately accessing or trying to access offensive or pornographic material | | | X | | | X | |  | |  | |  | | X | |
| Breaching copyright or licensing regulations | | |  | | |  | |  | | X | |  | |  | |
| Continued infringements of the above, following previous warnings or sanctions | | | X | | |  | |  | |  | | X | | X | |

### Acknowledgements

**The Scottish Government and 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 templates and of the 360 degree safe Scotland online safety self review tool:**

* Members of the SWGfL Online Safety Group
* Scottish Government and Education Scotland Officers
* Plymouth University Online Safety

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](http://www.antibullying.net/cyberbullying1.htm)) 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 January 2018. However, SWGfL cannot guarantee it’s accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2018

I know that if I break the rules I might not be allowed to use a computer/tablet.

## Social Media Policy

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

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents and carers and children / young people 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 and carers and children / young peoples.

### Scope

This policy is subject to the school’s codes of conduct and acceptable use policies.

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 children / young people 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’s 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 a personal social media account and such personal communications are outside the scope of this policy. However, where a personal account is used which associates itself with, or impacts on the school, this will be within the scope of the policy. It therefore must be made clear, with an appropriate disclaimer,that the member of staff is not communicating on behalf of the school.

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

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

### Organisational control

### Roles & Responsibilities

* The Head Teacher
  + 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
  + 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 school (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 he/she has posted via school accounts
  + adding an appropriate disclaimer to personal accounts when naming the school

### Monitoring

* **School accounts are monitored regularly and frequently** (including weekends and during holidays). Any comments, queries or complaints made through those accounts will 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 AUP.**
* **Digital communications by staff must be professional and respectful at all times and in accordance with this policy.** Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
* Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
* If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
* Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously 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 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 does not infringe upon relevant data protection laws, or breach confidentiality.

### Handling abuse

* When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
* If a conversation turns and becomes offensive or unacceptable, school users will block, report or delete other users or their comments/posts and will inform the audience exactly why the action was taken
* If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, 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 composing messages are:
* engaging
* conversational
* informative
* friendly (on certain platforms, eg. Facebook)

### 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 children / young people pictures online other than via school owned social media accounts or profiling tool.**
* Staff will exercise their professional judgement about whether an image is appropriate to share on school social media accounts.

### Personal use

### Staff

* personal communications are those made via a personal social media account. Where a personal communication associates itself with, or impacts on, the school, this will be within the scope of the policy unless the social media account contains an appropriate disclaimer which explains that the member of staff is not communicating on behalf of the school. Personal communications which do not refer to or impact upon the school are outside 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 the 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.*

### Children / Young People

* Staff are not permitted to follow or engage with current or prior children / young people of the school on any personal social media network account
* the school’s education programme should enable the children / young people to be safe and responsible users of social media
* children / young people 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 use Seesaw where posting or commenting is enabled, parents / carers will be informed about acceptable use
* the school has an active parent and carer education programme which supports the safe and positive use of social media. (Gooseberry Planet)
* parents and 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.

## Links to other organisations or documents

These may help give more information, should it be required;

**Scottish Government**

* [Digital Learning and Teaching](http://www.digital-literacy.org.uk/Home.aspx)
* [Glow](https://connect.glowscotland.org.uk/)
* [[Better relationships, better learning, better behaviour](http://www.scotland.gov.uk/Resource/0041/00416217.pdf‎)](https://www.education.gov.scot/improvement/inc52building-better-relationships)
* [National Action Plan on Internet Safety for Children and Young People](http://www.gov.scot/Publications/2017/04/1061)
* [Respect for All: The National Approach to Ant-bullying for Children and Young People](http://www.onlinecompass.org.uk)
* 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

* [Safer Internet Centre](http://www.saferinternet.org.uk/)
* [South West Grid for Learning](http://enable.eun.org/)
* [Childnet](http://www.childnet-int.org/)
* [Professionals Online Safety Helpline](mailto:onlinesafety@swgfl.org.uk)
* [Internet Watch Foundation](http://www.gov.scot/Topics/Education/Schools/ICTinLearning)

### CEOP

* [http://ceop.police.uk/](http://www.childnet.com/parents-and-carers)
* [ThinkUKnow](http://www.gov.scot/Publications/2017/11/6766)

**Others**

INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

* UK Council for Child Internet Safety (UKCCIS) - [www.education.gov.uk/ukccis](http://www.saferinternet.org.uk/about/helpline)
* Netsmartz - [http://www.netsmartz.org/index.aspx](https://www.iwf.org.uk/)

### Cyber/online bullying

* Scottish Anti-Bullying Service, respect*me* - [http://www.respectme.org.uk/](http://www.swgfl.org.uk/Staying-Safe)
* Scottish Government - [Better relationships, better learning, better behaviour](http://www.education.gov.uk/ukccis)
* Anti-Bullying Network - [http://www.antibullying.net/cyberbullying1.htm](http://www.saferinternet.org.uk)
* Cyberbullying.org - [http://www.cyberbullying.org/](http://ceop.police.uk/)
* Enable – EU funded anti-bullying project - [http://enable.eun.org/](http://www.thinkuknow.co.uk/)

### Sexting

* [UKCCIS - Sexting in schools and colleges: responding to incidents and safeguarding young people](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf)
* [UKSIC – Responding to and managing sexting incidents](http://swgfl.org.uk/magazine/Managing-Sexting-Incidents/Sexting-Advice.aspx)

### Social Networking

* Digizen – [Social Networking](http://digizen.org/socialnetworking/)
* [SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](https://www.education.gov.scot/improvement/inc52building-better-relationships)
* [UKSIC – Social Media Guides](http://www.netsmartz.org/index.aspx)

### Curriculum

53

* [SWGfL Digital Literacy and Citizenship Curriculum](http://www.cyberbullying.org/)

1. Glenbervie Primary- E-safety Policy updated December 2018 [↑](#footnote-ref-1)
2. See Personal Data Policy in the Appendix [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)
4. Authorised device – purchased by the pupil / family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school. [↑](#footnote-ref-4)
5. The school should add below any specific requirements about the use of mobile / personal devices in school [↑](#footnote-ref-5)