Bower Primary School



Online Safety

Policy

This policy applies to all members of the school community (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 made up of:

* Headteacher/senior staff
* Staff – including practitioners/support staff/
* Parents and carers
* Pupils

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

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

* Logs of reported incidents
* Surveys/questionnaires of
* Children / young people
* parents and carers
* staff

## 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 nursery, school, college or other setting**. 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.

### Headteacher and senior leaders:

* The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety may be delegated to the online safety co-ordinator/officer
* The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures).
* The headteacher/senior leaders are 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 headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety-net and also support to those colleagues who take on important monitoring roles.
* The headteacher/senior leaders will receive regular monitoring reports from the online safety co-ordinator/officer.

### Online safety co-ordinator/officer: Mrs Vicki Ross (principal teacher)

The online safety co-ordinator/officer:

* 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.
* meets with relevant officer (Robert Quigley) from the Local Authority to discuss current issues, review incident logs and if possible, filtering change control logs
* attends relevant meetings of pastoral care team / senior leadership team
* reports regularly to headteacher / senior leadership team

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

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.

Teaching and Support Staff

Are responsible for ensuring that:

* **they have an up to date awareness of online safety matters and of the current school online 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 headteacher or principal teacher.**
* **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
* in lessons where internet use is pre-planned 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

### Digital Leader – Principal Teacher

The digital leader 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 bullying

### Digital Leader Role

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

Members of the online safety group (or other relevant 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.
* the production / review / monitoring of the school filtering policy (if possible and if the school chooses to have one) and requests for filtering changes.
* mapping and reviewing 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’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 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, VLE, 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, VLE, 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 / VLE / 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**
* **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.
* 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.
* Children are only allowed on devices in the presence of an adult.
* 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
* Letters, newsletters, website, emails, learning platform, VLE
* 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/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers> (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, VLE, 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://www.onlinecompass.org.uk))

### 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 / officer (or other nominated person) will receive regular updates through attendance at external training events, (e.g. from SWGfL / 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 provision and control of digital infrastructure in the majority of Scottish schools will be the responsibility of respective local authorities..

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy/acceptable use policys. The school should also check their local authority / other relevant body policies on these technical issues if the service is not provided by the authority.

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:

* **All users will have clearly defined access rights to school technical systems and devices.**
* **All users, when deemed old enough / mature enough** (at approximately P3 and above) **will be provided with a username and secure password** by the class teacher who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
* **Internet access is filtered for all users. Illegal content (e.g. child sexual abuse; extreme pornography; criminally racist or terrorist content)** **is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.** (
* **Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet**.
* Where possible, school or 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 for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
* An agreed policy is in place 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.

### 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.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include: security risks in allowing connections to your school network; filtering of personal devices; breakages and insurance; access to devices for all children / young people; avoiding potential classroom distraction; network connection speeds, types of devices; charging facilities; total cost of ownership. A range of mobile technology implementations is possible.

For further reading, please refer to “Bring your own device: a guide for schools” by Alberta Education available at: <http://education.alberta.ca/admin/technology/research.aspx> and to the “NEN Technical Strategy Guidance Note 5 – Bring your own device” - <http://www.nen.gov.uk/bring-your-own-device-byod/>

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

* The school or local authority acceptable use policys for staff, children / young people, parents and carers will give consideration to the use of mobile technologies
* The school allows: (

|  |  |  |
| --- | --- | --- |
|  | School Devices | Personal Devices |
|  | School owned for individual use | School owned for multiple users | Authorised device[[3]](#footnote-3) | Owned by children / young people | Staff owned | Visitor owned |
| Allowed in school | Yes | Yes | Yes | Yes | Yes | Yes |
| Full network access | Yes | Yes | Yes |  |  |  |
| Internet only |  |  |  |  | 4G |  |
| No network access |  |  |  | yes |  | yes |

### 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.
* 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 come into force (General Data Protection Regulations – GDPR). ICO suggests: “It is essential to plan your approach to GDPR compliance now and to gain ‘buy in’ from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR’s new transparency and individuals’ rights provisions…… 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 will require organisations to review their approach to governance and how they manage data protection as a corporate issue. One aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organisations”.

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 policy 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 are clear policies 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:

|  |  |  |
| --- | --- | --- |
|  | 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  | yf yes |  |  |  |  |  |  |  |
| Use of mobile phones in lessons  | yes Yes |  |  |  |  |  |  |  |
| Use of mobile phones in social time |  |  |  |  |  |  |  |  |
| Taking photos on mobile phones / cameras | yes |  |  |  |  |  |  |  |
| Use of other mobile devices e.g. tablets, gaming devices  | yes |  |  |  |  |  |  |  |
| 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 |  |  |  |  |  |  |  |  |

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. Personal email addresses, text messaging or social media must not be used for these communications. Teaching staff should note that the General Teaching Council for Scotland has a Code of Professionalism and Conduct which all teachers are expected to adhere to. The code sets out the key principles and values for registered teachers in Scotland and Part 1 of the Code states the key features of the Professionalism of teachers and maintaining trust in the profession. One of the features is that registered teaches are mindful that social networking can blur the professional boundary between teacher and pupil and to avoid inappropriate communication (including via social networking) with young people under 18 years of age.
* Whole class/group email addresses may be used with younger children. While older children / 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.
* Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

### Social media

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully (online and/or offline), discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for children / young people and their families and for colleagues and the learning setting.

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
* The school permits reasonable and appropriate access to private social media sites

### 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.

### Unsuitable/inappropriate activities

Some internet activity, e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities, e.g. online bullying/hate crime would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in, or out of, school when using school equipment or systems. The school policy restricts usage as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| User Actions18 | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 |  |  |  |  | X |
| Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. |  |  |  |  | X |
| Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 |  |  |  |  | X |
| Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986  |  |  |  |  | X |
| Pornography |  |  |  | X |  |
| Promotion of any kind of discrimination |  |  |  | X |  |
| threatening behaviour, including promotion of physical violence or mental harm |  |  |  | X |  |
| Promotion of extremism or terrorism |  |  |  | X |  |
| Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute |  |  |  | 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 |  |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) |  |  |  | X |  |
| Creating or propagating computer viruses or other harmful files |  |  |  | X |  |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) |  |  |  | X |  |
| On-line gaming (educational) | x |  |  |  |  |
| On-line gaming (non-educational) |  |  | X |  |  |
| On-line gambling |  |  |  | X |  |
| On-line shopping / commerce |  |  |  | X |  |
| File sharing | X |  |  |  |  |
| Use of social media  |  |  |  | X |  |
| Use of messaging apps |  |  |  | X |  |
| Use of video broadcasting e.g. Youtube19 |  |  | x |  |  |

## 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 (see “User Actions” above).

### 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

|  |  |
| --- | --- |
|  | **Actions / Sanctions** |
| children / young people incidents | Refer to class teacher / tutor | Refer to Head of Department / Year / other | Refer to Headteacher / Principal | 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 detention / 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 |  | x |  |  | x |  |  |  |
| Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device | X |  | x |  |  | x |  |  |  |
| Unauthorised / inappropriate use of social media / messaging apps / personal email | x |  | x |  |  | x |  |  |  |
| Unauthorised downloading or uploading of files | x |  | x |  |  | X |  |  |  |
| Allowing others to access school network by sharing username and passwords | x |  |  |  |  |  |  |  |  |
| Attempting to access or accessing the school network, using another child’s / young person’s account | x |  | x |  |  | X |  |  |  |
| Attempting to access or accessing the school network, using the account of a member of staff | x |  | x |  |  | X |  |  |  |
| Corrupting or destroying the data of other users | X |  | x |  |  | X |  |  |  |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | x |  | x |  |  | x | x | x | X |
| Continued infringements of the above, following previous warnings or sanctions | x |  | 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 |  |  |  |
| Using proxy sites or other means to subvert the school’s filtering system | 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 |  | Xx | x | x | x |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act21 | x |  | x |  |  |  |  |  |  |
|  | **Actions / Sanctions** |
| Staff Incidents | Refer to line manager | Refer to Headteacher Principal  | 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 |  |  |  |  |  |  |
| Unauthorised downloading or uploading of files |  | 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 |  |  |  |  |  |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software |  | 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 |  |  |  |  |  |
| Using proxy sites or other means to subvert the school’s filtering system |  | x | X |  |  |  |  |  |
| Accidentally accessing offensive or pornographic material and failing to report the incident |  | X |  |  |  |  |  |  |
| Deliberately accessing or trying to access offensive or pornographic material |  | x | x | x | x | x | x | x |
| Breaching copyright or licensing regulations |  | x |  |  |  |  |  |  |
| Continued infringements of the above, following previous warnings or sanctions |  | 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) 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

#

# Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from the overview section of the 360 degree safe Scotland Online Safety Self Review Tool:

[www.360safescotland.org.uk](http://www.360safescotland.org.uk)

## Appendices – Section A - Acceptable use policy

* A1 Children / young people Acceptable use policy template (younger children)
* A2 Children / young people Acceptable use policy template (older children)
* A3 Staff and Volunteers Acceptable use policy template
* A4 Parents /Carers Acceptable use policy template
* A5 Community Users Acceptable use policy template

## Appendices – Section B – Specific Policies

* B1Technical Security Policy template
* B2 Personal Data Policy template
* B3 Mobile technologies policy template
* B4 Social media policy template
* B5 Online safety group terms of reference

## Appendices – Section C – Supporting documents and links

* C1 Responding to incidents of misuse – flowchart
* C2 Record of reviewing sites (for internet misuse)
* C3 Reporting log template
* C4 Training needs audit template
* C5 Summary of legislation
* C6 Links to other organisations and documents

## A1 Children / young people acceptable use policy template – for younger children [[4]](#footnote-4)

24

### This is how we stay safe when we use computers:

I will ask a teacher or another adult from the school if I want to use the computers

I will only use activities that a teacher or another adult from the school has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or another adult from the school if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or another adult from the school if I see something that upsets me on the screen.

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

**Signed (child):**

**Signed (parent):**

## A2 Children / young people acceptable use policy (AUP) template – for older children[[5]](#footnote-5)

### 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. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safer internet access at all times.

### This Acceptable Use Policy is intended to ensure:

* that children / young people will 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.

The school will try to ensure that children / young people will have good access to digital technologies to enhance their learning and will, in return, expect the children / young people to agree to be responsible users.

### Acceptable use

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

### For my own personal safety:

* I understand that the school will monitor my use of systems, devices and digital communications
* I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
* I will be aware of “stranger danger”, when I am communicating online
* I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, etc.)
* If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take an adult with me
* I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

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

* I understand that the school systems and devices are primarily intended for educational use and that I will only use them for personal or recreational use if I have permission
* I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, if I have permission
* I will only use the school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), if I have permission of a member of staff to do so.

25

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

* I will respect others’ work and property and will only access, copy, remove or alter any other user’s files, with the owner’s knowledge and permission
* I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
* I will only take or distribute images of others with their permission.

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

* I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
* I will immediately report any damage or faults involving equipment or software, however this may have happened
* I will only open hyperlinks in emails or attachments to emails, if I know and trust the person/organisation who sent the email, and have no concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
* I will only install/ store programmes on a school device, if I have permission

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

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

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

* I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information)
* I understand that if I fail to comply with this acceptable use policy, I will be subject to disciplinary action. This may include (s) loss of access to the school network/internet, contact with parents and in the event of illegal activities involvement of the police.

**Please complete the sections below / on the next page to show that you have read, understood and agree to the rules included in the acceptable use policy. If you do not sign and return this agreement, access will not be granted to school systems and devices.**

### Children / young people acceptable use policy

This form relates to the children / young people acceptable use policy, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use policy. If you do not sign and return this agreement, access will not be granted to school systems.

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

* I use the school systems and devices (both in and out of school)
* I use my own devices in the school (when allowed), e.g. mobile phones, gaming devices, cameras etc
* I use my own equipment out of the school in a way that is related to me being a member of this school, e.g. communicating with other members of the school, accessing school email, learning platform, website, etc.

Name of child / young person:

Group/Class

Signed:

Date:

### Parent/Carer Countersignature (optional)

Note: It is for schools to decide whether or not they require parents/carers to sign the Parent/carer acceptable use policy (see template later in this document). This includes a number of other permission forms (including digital and video images/biometric permission/cloud computing permission).

## A3 Staff (and volunteer) acceptable use policy template[[6]](#footnote-6)

### School policy

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

### This acceptable use policy is intended to ensure:

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

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

### Acceptable use

I understand that I must use school digital technologies 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 ICT for enhancing learning and will ensure that children / young people receive opportunities to gain from the use of digital technologies. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

### For my professional and personal safety:

* I understand that the school will monitor my use of the ICT systems, email and other digital communications.
* I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of 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.

28

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

* I will only access, copy, remove or alter any other user’s files, with 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/college’s policy on the use of digital/video images. I will only use my personal equipment to record these images, if I have permission to do so. Where these images are published, (e.g. on the school website/learning platform) it will not be possible to identify by name, or other personal information, those who are featured.
* I will only use chat and social networking sites in school in accordance with the school’s policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)
* I will only communicate with children / young people and parents/carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with children / young people and parents/carers. Staff should be made aware of the risks attached to using their personal email addresses/mobile phones/social networking sites for such communications)
* I will not engage in any online activity that may compromise my professional responsibilities.

### The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school :

* When I use my mobile devices laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
* I will not use personal email addresses on the school digital technology systems.
* I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (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, extremist material or 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 only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, with permission
* I will only install or attempt to install/store programmes on devices or if this is allowed in school policies.
* 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 protected and restricted data must be held in lockable storage.
* I understand that data protection policy requires that any staff or children / young people 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 the internet 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 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/local authority.
* I understand that if I fail to comply with this acceptable use policy, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Senior Management and/or the Local Authority 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 school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

## A4 Parent/carer acceptable use policy template[[7]](#footnote-7)

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

### This Acceptable Use Policy is intended to ensure:

* that young people will be responsible users and stay safe while 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.
* that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

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

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school’s work.

### Permission Form

Parent/Carers Name: Children / young person’s Name

As the parent/carer of the above children / young people, I give permission for my son/daughter to have access to the internet and to digital technology systems at school.

### Either: (Older children / young people)

I know that my son/daughter has signed an acceptable use policy and has received / will receive, online safety education to help them understand the importance of safe use of technology / internet – both in and out of school.

### Or: (younger children)

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

I understand that the school will take every reasonable precaution, including applying monitoring and filtering systems, to ensure that young people will be safe when they use the internet and digital technology systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son’s/daughter’s activity on the digital technology systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s online safety.

Signed Date:

### Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Children / young people and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with national guidance, 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.

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

### Digital/Video Images Permission Form

Parent/Carers Name:

Children / young people names:

As the parent/carer of the above children / young people(s), I agree to the school taking and using digital/video images of my child/children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

Yes/No

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes/No

Signed Date:

### Children / young people acceptable use policy

On the following pages we have copied, for the information of parents and carers, the children / young people acceptable use policy.



## C2 Record of reviewing devices/internet sites

(responding to incidents of misuse)

|  |  |
| --- | --- |
| Group |  |
| Date |  |
| Reason for investigation |  |

### Details of first reviewing person

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |

### Details of second reviewing person

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |

### Name and location of computer used for review (for web sites)

|  |
| --- |
|  |

### Web site(s) address/device Reason for concern

|  |  |
| --- | --- |
|  |   |
|  |  |
|  |  |
|  |  |
|  |  |

### Conclusion and action proposed or taken

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |
| --- |
| C3 Reporting Log TemplateGroup:  |
| Date | Time | Incident | Action Taken | Incident Reported By | Signature |
| What? | By Whom? |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| C4 Training Needs Audit Log TemplateGroup:  |
| Relevant training the last 12 months | Identified Training Need | To be met by | Cost | Review Date |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## C5 Summary of Legislation

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

### Computer Misuse Act 1990

This Act makes it an offence to:

* erase or amend data or programs without authority;
* obtain unauthorised access to a computer;
* “eavesdrop” on a computer;
* make unauthorised use of computer time or facilities;
* maliciously corrupt or erase data or programs;
* deny access to authorised users.

### Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

* fairly and lawfully processed.
* processed for limited purposes.
* adequate, relevant and not excessive.
* accurate.
* not kept longer than necessary.
* processed in accordance with the data subject’s rights.
* secure.
* not transferred to other countries without adequate protection.

### Freedom of Information (Scotland) Act 2000

The Freedom of Information (Scotland) Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information (Scotland) Act. When responding to requests, they have to follow a number of set procedures.

### Communications Act 2003

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

### Malicious Communications Act 1988

It is an offence to send an indecent, grossly offensive, or threatening letter, electronic communication or other article to another person. It is also an offence to send information which is false and known or believed to be false by the sender.

### Regulation of Investigatory Powers (Scotland) Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Where the system controller has given express consent monitoring or keeping a record of any form of electronic communications is permitted, in order to:

* establish the facts;
* ascertain compliance with regulatory or self-regulatory practices or procedures;
* demonstrate standards, which are or ought to be achieved by persons using the system;
* investigate or detect unauthorised use of the communications system;
* prevent or detect crime or in the interests of national security;
* ensure the effective operation of the system.
* monitoring but not recording is also permissible in order to:
* ascertain whether the communication is business or personal;
* protect or support help line staff

### Trade Marks Act 1994

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

### Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

### Criminal Justice & Public Order Act 1994 / Public Order Act 1986

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

* use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
* display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

### Racial and Religious Hatred Act 2006 / Public Order Act 1986

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

### Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

### Protection of Children Act and Prevention of Sexual Offences (Scotland) Act 2009

This legislation introduced a new offence of sexual grooming of a person under 16; It also introduces Risk of Sexual Harm Orders (RSHOs) which are designed to protect children from those who display inappropriate behaviour towards them; It introduces a new offence of paying for the sexual services of a person under 18; It introduces new offences of causing, inciting, controlling, arranging or facilitating the provision of sexual services by children or child pornography; It amends current legislation criminalising the taking, possessing and distribution of indecent images of children so that it applies to images of people under 18 rather than only to images of those under 16.

### Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

### Obscene Publications Act 1959 and 1964

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

### Human Rights Act 1998

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

* the right to respect for private and family life, home and correspondence
* freedom of thought, conscience and religion
* freedom of expression
* freedom of assembly
* prohibition of discrimination
* the right to education
* the right not to be subjected to inhuman or degrading treatment or punishment

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

#### Children and Young People (Scotland) Act 2014

#### Education Scotland Act 2016

#### Standards in Scotland’s Schools Etc Act 2000

Includes framework for school improvement planning and inspection.

#### Scottish Schools Parental Involvement Act 2006

Guidance on promotion of parental involvement in schools.

#### [Offensive Behaviour at Football and Threatening Communications (Scotland) Act 2012](http://www.scottish.parliament.uk/parliamentarybusiness/CurrentCommittees/31384.aspx)

Focuses on behaviour at Football matches, but also **criminalises the communication of threats of serious violence and threats intended to incite religious hatred, whether sent through the post or posted on the internet.** The Act will only criminalise behaviour likely to lead to public disorder which expresses or incites hatred, is threatening or is otherwise offensive to a reasonable person.

#### Equality Act 2010

UK Government legislation applicable to Scotland. Reforms and harmonises equality law and restates previous legislation relating to discrimination and harassment related to seven personal characteristics: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex, and sexual orientation.

## C7 Links to other organisations or documents

These may help those who are developing or reviewing an online safety policy.

### Scottish Government

* [Digital Learning and Teaching](http://www.gov.scot/Topics/Education/Schools/ICTinLearning)
* [Glow](https://connect.glowscotland.org.uk/)
* [[Better relationships, better learning, better behaviour](http://www.scotland.gov.uk/Resource/0041/00416217.pdf%E2%80%8E)](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.gov.scot/Publications/2017/11/6766)
* 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://www.swgfl.org.uk/Staying-Safe)
* [Childnet](http://www.childnet-int.org/)
* [Professionals Online Safety Helpline](http://www.saferinternet.org.uk/about/helpline)
* [Internet Watch Foundation](https://www.iwf.org.uk/)

### CEOP

* <http://ceop.police.uk/>
* [ThinkUKnow](http://www.thinkuknow.co.uk/)

### 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.education.gov.uk/ukccis)
* Netsmartz - <http://www.netsmartz.org/index.aspx>

### Cyber/online bullying

* Scottish Anti-Bullying Service, respectme - <http://www.respectme.org.uk/>
* Scottish Government - [Better relationships, better learning, better behaviour](https://www.education.gov.scot/improvement/inc52building-better-relationships)
* Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>
* Cyberbullying.org - <http://www.cyberbullying.org/>
* Enable – EU funded anti-bullying project - <http://enable.eun.org/>

### 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](http://360safe.org.uk/Files/Documents/facebook-6)
* [UKSIC – Social Media Guides](https://www.saferinternet.org.uk/advice-centre/social-media-guides)

### Curriculum

53

* [SWGfL Digital Literacy and Citizenship Curriculum](http://www.digital-literacy.org.uk/Home.aspx)
* Teach Today – [www.teachtoday.eu/](http://www.teachtoday.de/en/)
* Insafe - [Education Resources](http://lreforschools.eun.org/web/guest/insafe)

### Mobile Devices/BYOD

53

NEN - [Guidance Note - BYOD](http://www.360safe.org.uk/Files/Documents/NEN_Guidance_Note_5_BYOD.aspx)

### Data Protection

* Scottish Government / Scottish Information Commissioners Office:

[Biometric recognition technology in schools advice note](http://www.scotland.gov.uk/Publications/2010/11/11112141/0)

[Its public knowledge](http://www.itspublicknowledge.info/ScottishPublicAuthorities/ScottishPublicAuthorities.aspx) (guidance for public authorities on FOI)

* Information Commissioners Office:
* [Your rights to your information – Resources for Schools - ICO](http://www.ico.org.uk/schools)
* [ICO pages for young people](https://ico.org.uk/for-organisations/education/resources-for-schools/infographic/)
* [Guide to Data Protection Act - Information Commissioners Office](https://ico.org.uk/for-organisations/guide-to-data-protection/%22%20%5Ct%20%22_blank)
* [Guide to the Freedom of Information Act - Information Commissioners Office](https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/)
* [ICO - Guidance we gave to schools - September 2012 (England)](https://ico.org.uk/media/for-organisations/documents/1132/report_dp_guidance_for_schools.pdf%22%20%5Ct%20%22_blank)
* [ICO Guidance on Bring Your Own Device](https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf%22%20%5Ct%20%22_blank)
* [ICO Guidance on Cloud Computing](https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf%22%20%5Ct%20%22_blank)
* [Information Commissioners Office good practice note on taking photos in schools](http://360safe.org.uk/Files/Documents/ICO-Good-Practice-Note-on-taking-photos-in-schools%22%20%5Ct%20%22_blank)
* [ICO Guidance Data Protection Practical Guide to IT Security](http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/it_security_practical_guide.ashx)
* [ICO – Think Privacy Toolkit](http://www.ico.org.uk/for_organisations/training/think-privacy-toolkit)
* [ICO – Personal Information Online – Code of Practice](http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/personal_information_online_cop.ashx)
* [ICO Subject Access Code of Practice](http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.PDF)
* [ICO – Guidance on Data Security Breach Management](http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/guidance_on_data_security_breach_management.pdf)
* NEN - [Guidance Note - Protecting School Data](http://www.360safe.org.uk/Files/Documents/NEN_Guidance_Note_1_protecting_school_data.aspx)

### Professional Standards/Staff Training

General Teaching Council Scotland: <http://www.gtcs.org.uk/standards/copac.aspx>

* [Kent - Safer Practice with Technology](https://www.kscb.org.uk/guidance/online-safety)
* [Childnet/TDA - Social Networking - a guide for trainee teachers & NQTs](http://www.childnet.com/resources/social-networking-a-guide-for-teachers-and-professionals%22%20%5Ct%20%22_blank)
* [Childnet/TDA - Teachers and Technology - a checklist for trainee teachers & NQTs](http://www.childnet.com/resources/teachers-and-technology-checklist%22%20%5Ct%20%22_blank)
* [UK Safer Internet Centre Professionals Online Safety Helpline](https://www.saferinternet.org.uk/professionals-online-safety-helpline%22%20%5Ct%20%22_blank)

### Infrastructure/Technical Support

* Somerset - [Questions for Technical Support](http://www.360safe.org.uk/Files/Documents/Questions-for-Technical-Support-Somerset.aspx)
* NEN **-** [E-security: Managing and maintaining e-security/ cyber security in schools](http://www.nen.gov.uk/advice/e-security-managing-and-maintaining-e-security-cyber-security-in-schools)
* [NEN –School e-Security Checklist](http://www.nen.gov.uk/advice/school-e-security-checklist)

### Working with parents and carers

* Education Scotland’s parentzone <https://education.gov.scot/parentzone/>
* National parent Forum of Scotland <https://www.npfs.org.uk/>
* Scottish Parent Teacher Council https://www.sptc.info/
* [Parenting across Scotland](http://www.parentingacrossscotland.org/info-for-families/hot-topics/online-safety/)
* Parentline - <https://www.children1st.org.uk/what-we-do/how-we-help/parentline-scotland/>
* [Vodafone Digital Parents Magazine](http://www.vodafone.com/content/digital-parenting.html/%22%20%5Ct%20%22_blank)
* [Childnet Webpages for Parents & Carers](http://www.childnet.com/parents-and-carers%22%20%5Ct%20%22_blank)
* [Get Safe Online - resources for parents](http://www.getsafeonline.org/nqcontent.cfm?a_id=1182" \t "_blank)
* [Teach Today - resources for parents workshops/education](http://www.teachtoday.de/en/%22%20%5Ct%20%22_blank)
* [The Digital Universe of Your Children - animated videos for parents (Insafe)](https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=198334)
* [Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](http://www.360safe.org.uk/Files/Documents/Learning-Disabilities%2C-Autism-and-Internet-Safety.aspx)
* [Internetmatters.org](https://www.internetmatters.org/)

### Research

* [Futurelab - "Digital participation - its not chalk and talk any more!"](http://360safe.org.uk/Files/Documents/FutureLab-Digital-participation--its-not-chalk-and)
* [Social Media and Children’s Mental Health – a review of the evidence – Education Policy Institute 2017](https://epi.org.uk/report/social-media-and-childrens-mental-health-a-review-of-the-evidence/)

56

54

57

* [UK Safer Internet Centre (SID 2017) Research – the Power of Image](https://www.saferinternet.org.uk/safer-internet-day/2017/power-of-image-report)

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 January 2018 . 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.

1. [↑](#footnote-ref-1)
2. See Personal Data Policy in the Appendix [↑](#footnote-ref-2)
3. 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-3)
4. Consultation with the local authority officer responsible for the acceptable use policy is advised to ensure your school is following local authority policy. [↑](#footnote-ref-4)
5. Consultation with the local authority officer responsible for the acceptable use policy is advised to ensure your school is following local authority policy. [↑](#footnote-ref-5)
6. Consultation with the local authority officer responsible for the acceptable use policy is advised to ensure your school is following local authority policy. [↑](#footnote-ref-6)
7. Consultation with the local authority officer responsible for the acceptable use policy is advised to ensure your school is following local authority policy. [↑](#footnote-ref-7)