



Midmar School

Online Safety Policy

June 2022

Article 17: (access to information from the media) Every child has the right to reliable information from a variety of sources, and governments should encourage the media to provide information that children can understand. Governments must help protect children from materials that could harm them.

Article 19: (protection from violence, abuse and neglect). Governments must do all they can to ensure that children are protected from all forms of violence, abuse, neglect and bad treatments by their parents or anyone else who looks after them.

Article 28: (Right to education) Every child has the right to an education. Primary education must be free. Discipline in schools must respect children's dignity and their rights.

Article 29: (goals of education) Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human right, as well as respect for their parents, their own and other cultures and the environment.

Article 31: (Leisure, play and culture) Every child has the right to relax, play and take part in a wide range of cultural and artistic activities.

Article 34: (sexual exploitation) Governments must protect children from all forms of sexual abuse and exploitation.

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

This online safety policy has been developed by Technology Group and a working party made up of

- Headteacher
- Staff – teaching and non-teaching
- Learners
- Parents

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

Schedule for Development/Monitoring/Review

| | |
|---|--|
| This online safety policy was agreed: | 29.6.22 |
| The implementation of this online safety policy will be monitored by the: | Head Teacher and Technology Group – supported by Mrs Sutherland |
| Monitoring will take place at regular intervals: | Termly – October, December, March, July |
| The <i>Headteacher</i> will receive a report on the implementation of the online safety policy generated by the Technology Group (which will include anonymous details of online safety incidents) at regular intervals: | Termly – October, December, March, June |
| The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | 1 st June 2023 |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | Aberdeenshire Council, IT Support Paul Cruickshank QIO Child Protection lead – E. Shepherd Duty Social Work Team – Kemnay and Westhill Grampian Police |

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited) - Aberdeenshire Council*
- *Surveys/questionnaires of*
 - *Children / young people*
 - *parents and carers*
 - *staff*

Scope of the Policy

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 individuals¹ 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.
- The headteacher 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 is responsible for ensuring that the online safety co-ordinator 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 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 support to those colleagues who take on important monitoring roles.
- The headteacher will receive regular monitoring reports from the online safety co-ordinator.

Online safety co-ordinators: Mrs E Shepherd (Head Teacher), Mrs G Sutherland (Teacher)

The online safety co-ordinators

- lead the online safety group
 - take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
 - ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
 - ensure they are up to date with national relationships and behaviour guidance and anti-bullying guidance
 - provide (or identifies sources of) training and advice for staff
 - record incidents of online bullying through the school's SEEMiS recording system in line with local procedures
 - liaise with the local authority/relevant body
 - receive reports of online safety incidents and creates a log of incidents to inform future online safety developments.
-

- meet regularly with relevant officer from the Local Authority to discuss current issues, review incident logs and if possible, filtering change control logs

Designated Getting it Right for Every Child - Named Person: Mrs E Shepherd (Head Teacher)

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

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

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

Network manager/technical staff:

The Local Authority is responsible for ensuring:

- that the school technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body and also the online safety policy / guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as appropriate.
- that the use of the network / internet / learning platform / VLE / remote access / email is regularly monitored in order that any misuse/attempted misuse can be reported to the headteacher.
- that (if present) monitoring software/systems are implemented and updated as agreed in school policies
- that the filtering policy, is applied and updated on a regular basis and its implementation is not the sole responsibility of any single 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; online safety co-ordinator / officer* for investigation / action
- all digital communications with children / young people/parents and carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities using the refreshed curriculum guidance in the Technologies experiences and outcomes.
- children / young people understand and follow the online safety and acceptable use policies
- children / young people have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *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*

Child Protection Coordinator : Mrs E Shepherd (Head Teacher)

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

- sharing of personal data²
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying

Online safety group (Technology Group)

The Technology Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives.

Members of the Technology Group will assist the online safety co-ordinators with:

- the production / review / monitoring of the school online safety policy / documents in line with local anti-bullying policies.
- 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

² See Personal Data Policy in the Appendix

- 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)
- *Respectme*, Scotland's anti-bullying service, deliver training for parents and carers with a focus upon how they can best support their children and young people in their relationships with online technology which includes access to practical advice relating to online settings and security. www.respectme.org.uk

Policy Statements

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.
- 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.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 (Cyber Resilience -ALDO) 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 policies.**
- The online safety co-ordinator 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-ordinators will provide advice / guidance / training to individuals as required.

Technical – infrastructure/equipment, filtering and monitoring

Midmar School will work closely with Aberdeenshire Council to ensure that the school's digital infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by class teachers / administrator *who will keep an up-to-date record of users and their usernames*. Users are responsible for the security of their username and password *and will be required to update their password every academic year*.
- The “master/administrator” passwords for the school digital systems, used by the network manager (or other person) must also be available to the headteacher and kept in a secure place, (e.g. school safe)
- Linda Keir – Administrator is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. 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. There is a clear process in place to deal with requests for filtering .
- 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. Users will report incidents to Mrs Sutherland or Mrs Shepherd. They will be recorded in the Incident Log.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software. (Aberdeenshire systems).
- An agreed policy is in place for the provision of temporary access of “guests”, (e.g. trainee teachers, supply teachers, visitors) onto the school systems. School will have a ‘guest’ login.
- 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. – Not applicable at present as no school devices do not go home. (June 2022).
- An agreed policy is in place that allows forbids staff from downloading executable files and installing programmes on school devices – only Aberdeenshire IT staff can install programmes.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile technologies

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

All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies 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/>

At Midmar School we use the Aberdeenshire Acceptable Use Policy. The main points from this policy.

- The school or local authority acceptable use policy 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 | Owned by children / young people | Staff owned | Visitor owned |
| Allowed in school | Yes | Yes | No | No ⁴ | No ⁸ | No ⁸ |
| Full network access | Yes | Yes | No | No | No | No |
| Internet only | Yes | Yes | No | No | No | No |
| No network access | No | No | No | No | No | No |

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.

⁴ The school should add below any specific requirements about the use of mobile / personal devices in school

School owned/provided devices:

- Individual pupils will be allocated devices. HT and teachers will be allocated devices.
- Devices will be stored in locked cabinets in the GP Hall. Children can access devices throughout the day on the instruction of teachers. Teachers carry their tablets in school and home.
- Personal use is not allowed.
- Children can access Aberdeenshire network and the internet – supervised by teachers / PSA. Levels of access to networks/internet
- Children can use the 'Self Service' app. to find / install apps. Children should not be changing settings unless directed to by teachers.
- Network/broadband capacity - set by Aberdeenshire Council and is currently appropriate.
- Technical support is provided by Aberdeenshire Council
- Filtering of devices – filters are set by Aberdeenshire Council
- Access to cloud services
- Data Protection
- Taking/storage/use of images – always ask the person being photographed if they are happy to have their picture taken, explain the purpose of the photograph. Images should be stored up to 5 years, Images will be stored centrally by teachers. All parents have indicated their preferences – regarding children being photographed.
- Exit processes – if an adult or child leaves the school their device will be reset to factory settings. Any images / information will be moved / saved
- Liability for damage – users are liable for any damage caused to a device.
- Staff training – a programme for staff training is provided by Aberdeenshire Council.

Personal devices: Currently personal devices are not allowed in school

- Which users are allowed to use personal mobile devices in school (staff /children / young people / visitors/parents and carers?)
- Restrictions on where, when and how they may be used in school
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks / internet (as above)
- Network / broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- Taking / storage / use of images
- Liability for loss / damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification / labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

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: ([select/delete as appropriate](#))

- 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 is 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- Aberdeenshire Acceptable User Agreement
- 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.

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
- The Head Teacher has overall responsibility for ensuring that the school complies with authority guidance and /or Data Protection Act in their handling of data, and who identifies and responds to risks related to handling of personal data; risk assessments are carried out. All staff must complete Data Protection training every two years.
- 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
- the data must be securely deleted from the device, in line with Aberdeenshire Policy once it has been transferred or its use is complete

Communications

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree how they intend to implement and use these technologies, e.g. some schools do not allow children / young people to use mobile phones in lessons, while others identify educational potential and allow their use. This section may also be influenced by the age of the children / young people. The table has been left blank for school to choose its own responses.

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:

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

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 teachers 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

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 Actions

| | | 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 | | |

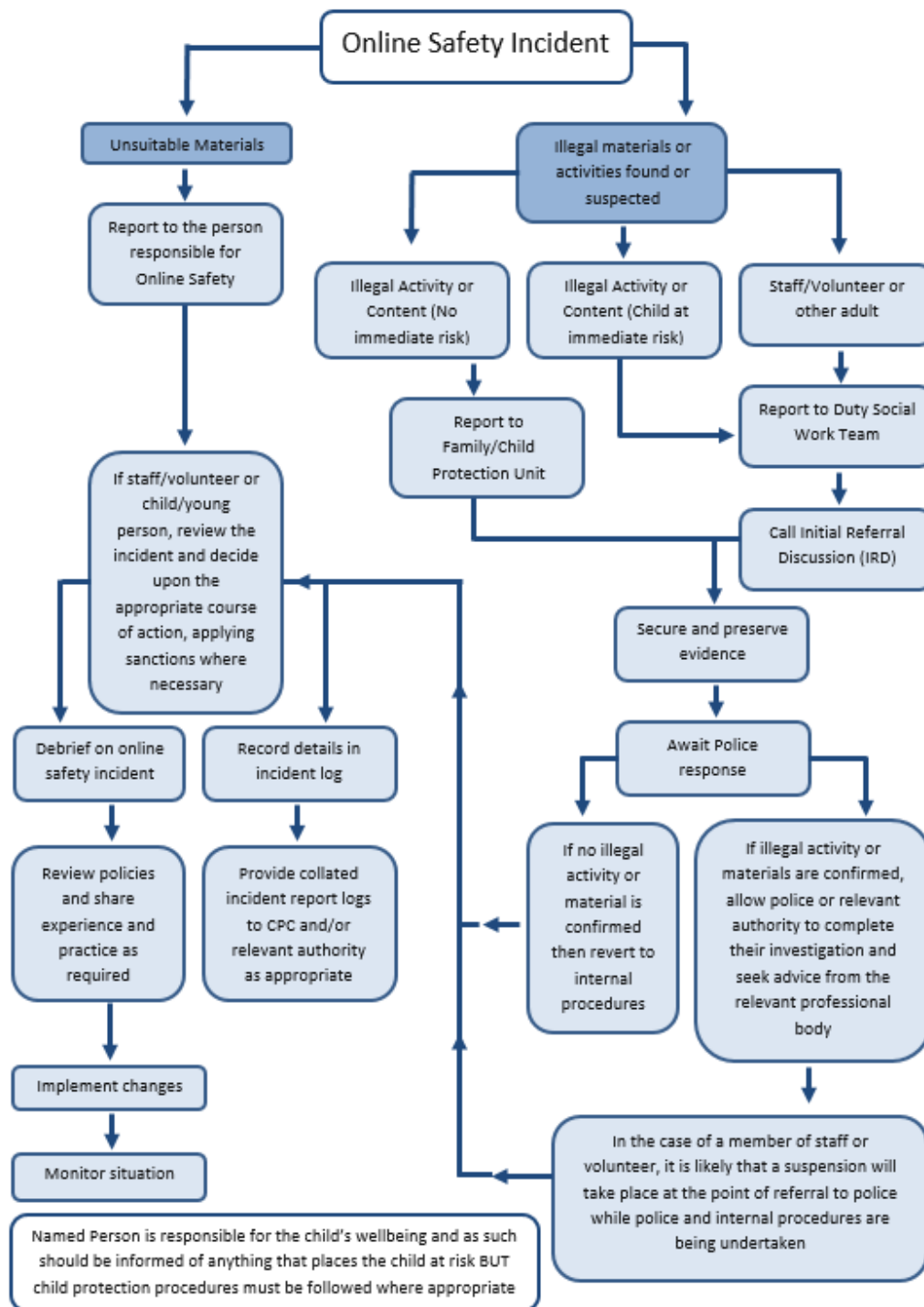
| | | | | | |
|---|--|---|---|---|--|
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | | | | X | |
| On-line gaming (educational) | | X | | | |
| On-line gaming (non-educational) | | | | X | |
| On-line gambling | | | | X | |
| On-line shopping / commerce | | | | X | |
| File sharing | | X | | | |
| Use of social media | | X | | | |
| Use of messaging apps | | | | X | |
| Use of video broadcasting e.g. Youtube | | | 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 co-ordinator – Mrs Sutherland | 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 | X | | |
| Unauthorised use of non-educational sites during lessons | X | X | X | | | X | | X | |
| Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device | X | X | X | | | X | | X | |
| Unauthorised / inappropriate use of social media / messaging apps / personal email | X | X | X | | | X | | X | |
| Unauthorised downloading or uploading of files | X | X | X | | | X | | X | |
| Allowing others to access school network by sharing username and passwords | X | X | X | | | | | X | |
| Attempting to access or accessing the school network, using another child's / young person's account | X | X | X | | | | | X | |
| Attempting to access or accessing the school network, using the account of a member of staff | X | X | X | | | | | X | |
| Corrupting or destroying the data of other users | X | X | X | | | | | X | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | | | X | | X | |

| | | | | | | | | | |
|---|---|---|---|--|--|--|---|---|---|
| Continued infringements of the above, following previous warnings or sanctions | | | | | | | | X | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | X | X | | | | X | | X |
| Using proxy sites or other means to subvert the school's filtering system | X | X | X | | | | X | | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | X | | | | X | X | |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | X | | | | X | X | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | X | X | X | | | | X | | X |

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 | | X | | X |
| Inappropriate personal use of the internet / social media / personal email | | X | X | | | X | | X |
| Unauthorised downloading or uploading of files | | X | X | | | | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | | X | X | | | X | | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | | X | X | | | X | | X |

| | | | | | | | |
|---|---|---|--|---|--|---|---|
| Deliberate actions to breach data protection or network security rules | X | X | | | | X | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | X | X | | | | X | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | | | | X | X |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with children / young people | X | X | | | | | X |
| Actions which could compromise the staff member's professional standing | X | X | | | | X | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | X | | | | X | X |
| Using proxy sites or other means to subvert the school's filtering system | X | X | | X | | X | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | | X | | X | |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | | | | X | X |
| Breaching copyright or licensing regulations | X | X | | X | | X | |
| Continued infringements of the above, following previous warnings or sanctions | X | X | | | | X | X |
| | | | | | | | |

Acknowledgements

The Scottish Government and SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this school online safety policy templates and of the 360 degree safe Scotland online safety self review tool:

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

Copyright of these policy templates is held by SWGfL. Schools and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) 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 November 2017. However, SWGfL cannot guarantee it's accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2018

This Policy was compiled by pupils, staff and parents. June 2022

Head Teacher: Elizabeth Shepherd

Teachers: Gemma Sutherland, Jayne Miller, Anne Reid

Support Staff: Mairi Black, Linda Keir, Shelley McCullach

Parents: Lesley Tierney, Sandra Jaffrey

Technology Group