Macduff Primary School

Online Safety Policy

Content

Introduction

Technology is seen as a fundamental resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. In order to build the skills for today, tomorrow and the future and better prepare our young people for lifelong learning and work, we need to incorporate the use of technology into our curriculum. At Banff Academy we are committed to ensuring that children learn how to use computers, ICT and modern technologies safely so that they:

- Are able to use ICT safely to support their learning
- Know how to use a range of ICT equipment
- Are able to use ICT and technologies outside of school safely
- Are prepared for the constant evolution of technology and can adapt their skills for the future

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 the Online Safety Group made up of:

- *Senior Leadership*
- *Online safety officer*
- *Staff*
- *Pupils*

Schedule for Development/Monitoring/Review

This online safety policy was agreed:	*14/06/19*
Implementation will be monitored by:	*The Online Safety Group*
Monitoring will take place at regular intervals:	*Annually in term 4 along with newsletter*
The *Senior Leadership Team* will receive a report on the implementation of the online safety policy:	*Annually*
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:	*07/06/19*
Should serious online safety incidents take place, the following persons should be informed:	*Child Protection Officer/Principal Teacher of Guidance*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Internal monitoring data for network activity*
- *Surveys/questionnaires of young people, parents, carers and staff*

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Local Authority:

The school will work very closely in partnership with officers from Aberdeenshire Council to ensure that the schools' 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 SLT members
- 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.
- The Headteacher is responsible for ensuring staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The headteacher/senior leaders will receive regular monitoring reports from the online safety co-ordinator/officer and *Learning Through Technology* leadership group.
- The Headteacher meets with *Learning Through Technology* team to discuss current issue.

Child Protection Officer/ Online Safety Officer

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

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Online bullying.

The online safety officer:

- Is part of 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 needs to be followed in the event of an online safety incident taking place.
- Provides (or identifies sources of) training and advice for staff.
- 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.
- Attends relevant meetings of pastoral care team / senior leadership team.
- Reports regularly to headteacher / senior leadership team.

Aberdeenshire Council ICT:

- Aberdeenshire Council is responsible for ensuring:
- The school technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required e-safety technical requirements.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation and action.

Technical – infrastructure / equipment, filtering and monitoring

Aberdeenshire Council will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

The school will therefore monitor the activities of users on the school network and on school equipment as indicated in this policy and the Acceptable Use agreement.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- ICT are 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.
- Internet access is filtered for all users. Illegal content (e.g. child sexual abuse images) 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 regularly monitored. There is a clear process in place to deal with requests for filtering changes. Differentiated user-level allows filtering levels for different ages / stages and different groups of users.
- An appropriate system is in place for users to report any actual / potential e-safety incident to the E-Safety Coordinator / Network Manager / Technician (or other relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place that allows staff to / forbids staff from installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Network manager/technical staff:

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

- That the school technical infrastructure is secure and is not open to misuse or malicious attack

- That the 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 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 / senior leader; online safety co-ordinator for investigation / action / sanction.
- 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 / senior leader/ online safety co-ordinator 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.
- 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.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. The group will also be responsible for regular reporting to senior leadership team. The Online Safety Group consists of the Learning Through Technology Leadership Group, members of the Senior Leadership Team, IT Technicians, and the Online Safety Officer.

Members of the Online Safety Group will assist the Online Safety Co-ordinator with:

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

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 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.

Mobile Technologies

Pupils will be able to use mobile technology devices in school in order to assist in their learning. Mobile technology devices will be a school provided, 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's/college's learning platform and other cloud-based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the staff and wider school community understand that the primary purpose of having a device at school is educational. The mobile technologies policy will sit alongside a range of polices including but not limited to the safeguarding policy, anti-bullying policy, policies around theft or malicious damage and the behaviour policy.

Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Children / young people now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen learning, but they can also develop digital literacy, fluency and citizenship in children / young people that will prepare them for the high-tech world in which they will live, learn and work.

Personal devices

We do not permit children to bring their own devices to school as we provide sufficient access to school ICT that the benefits of bringing a device are not outweighed by the risks.

For adults who are permitted to use a personal device:

- All personal devices are restricted through filtered network access.

- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents / carers) as does the liability for any loss or damage resulting from the use of the device in the school.
- Staff personal devices should not be used to contact children / young people or their families, nor should they be used to permanently store images of children / young peoples.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at the school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school recommends that the devices are made easily identifiable, have a protective case and are secured with a pass-code or pin.
- The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.
- Personal devices should be charged before being brought to the school as the charging of personal devices may not be permitted during the school day.

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by ICT. They will manage the school filtering, in line with this policy and will keep records / logs of changes.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service will be logged in change control logs.

All users have a responsibility to report immediately to ICT any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programs or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by ICT. Illegal content is filtered by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet

access through the council's network infrastructure, filtering will be applied that is consistent with school practice.

- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher or other nominated senior leader.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
- Any filtering issues should be reported immediately to ICT.
- Requests from staff for sites to be removed from the filtered list will be considered by ICT, Liaising with the ECS Technology Development Manager where appropriate

Education / Training / Awareness

Children / young people will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- The Acceptable Use Agreement.
- Induction training.
- Staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to ICT.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use agreement.

Audit / Reporting

Logs of filtering change controls will be made available to the ECS Technology Development Manager on request.

User Behaviour

Users are expected to act responsibly, safely and respectfully in line with current acceptable use policies, in addition where applicable;

- **The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the behaviour policy.**
- **Guidance is made available by the school to users concerning where and when mobile devices may be used.**
- **Devices may not be used in tests unless directed by a teacher.**
- **Users are responsible for keeping their device up to date through software, security and app updates. The device has to be virus protected and should not be capable of passing on infections to the network.**
- **Users are responsible for charging their own devices and for protecting and looking after devices belonging to school.**
- **Users should be mindful of the age limits for apps and use and should ensure they read the terms and conditions before use.**
- **Children / young people must only photograph people with their permission and must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately.**
- *Devices may be used in lessons in accordance with teacher direction.*

Unsuitable/inappropriate activities

Some internet activity, e.g. accessing child abuse images or distributing racist material is illegal and is banned from school and all other technical systems. Other activities, e.g. online bullying/hate crime is banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but are 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) 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 involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the investigation 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

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:

User incidents	Warning	Refer to class teacher	Confiscation of device	Reefer to head of department	Refer to DHT	Refer to police (DHT)	Inform Parents/carers	Refer to technical support staff for 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
Deliberately accessing or trying to access offensive or pornographic material					X	X	X	X
Deliberate unauthorised downloading or uploading of inappropriate files					X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident					X		X	X
Using proxy sites or other means to subvert the school's filtering system					X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		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	
Attempting to access a school device using the account of a member of staff					X			
Corrupting or destroying the data of other users		X		X	X			
Malicious attempt to use another users device					X		X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act					X			
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X	X					
Inappropriate use of social media / messaging apps / personal email	X	X	X					
Unauthorised use of non-educational sites during lessons	X	X	X					