Annan School

E-Safety and ICT Acceptable Use Policy

Version: 09/23
Effective Date: September 2023

Reviewed by: Debby Hunter
Reviewed on: 13/06/23

E-SAFETY AND ICT ACCEPTABLE USE POLICY

Our e-Safety Policy has been written by the school, specifically in relation to the School's Child Protection and Safeguarding Policy of which it should be seen as an integral part.

The policy is accompanied by two documents for guidance:

- *Appendix 1: Mobile Phone Use Staff Guidance*
- *Appendix 2: Camera, Photograph And Social Networking Guidance*

This policy specifically includes the Early Years Foundation Stage (EYFS).

The e-Safety Policy applies to both pupils and staff at the school. Where a section of the policy applies solely to either pupils or members of staff this is indicated above the relevant section, otherwise it applies to all users.

In this policy the term 'Principal' applies to Debby Hunter.

Links to Statutory Guidelines referred to in this document can be found in the main Child Protection and Safeguarding Policy

1. E-SAFETY POLICY

Teaching and Learning

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

Internet use is a part of the curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content, or extremist material by immediately reporting it to their teacher. This will also allow the teacher to assess if there has been a breach of the school's filtering system.
- Internet safety is an integral part of the school's ICT curriculum and is embedded in the Personal Social, Health and Economic curriculum(PSHE). It is also included in the school's commitment to the ***Prevent*** strategy.
- Pupils will take part in discrete safety lessons appropriate to the age of the children.

Managing Internet Access and Safety

- We take a 'whole school approach to on-line safety'.
- The school will ensure appropriate filters are in place to safeguard pupils from potentially harmful and inappropriate material on-line, but without an unreasonable level of blocking.
- The search engine used by pupils in the school is Microsoft Edge. This has Bing safe search filters set up and is has been assessed as the most appropriate for use at the school. All Microsoft Edge searches go through a central school account which is monitored by the school. Currently Lucie Hunter is responsible for keeping the search filters up to date and monitoring the searches being made on school laptops.
- The school will consider its duty in response to the ***Prevent*** strategy to make appropriate provision to prevent pupils being influenced or targeted to participate in radicalism or extremism.
- Pupils are not allowed access to personal 3G, 4G and 5G enabled devices on school premises, or during school activities, unless by agreement with the Principal (i.e. in the case of SEND or EAL)
- The school follows guidance such as that produced the **UK Safer Internet Centre**: Internet Safety: appropriate filtering and monitoring and guidance on e-security available from National Education Network (NEN)

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.

Social networking and personal publishing (pupils)

- The school network has in place controlled access to websites accessed via the school internet. This includes access to social networking sites.
- Pupils have access to the MS Teams Portal - Blick! Pupils are not permitted to use the individual 'chat' facility within Blick and where possible this will be disabled. Pupils are able to communicate via their class Blick! channels through 'posts'. These are open 'posts' and can be read by all members of the channel including staff. However 'agreed rules' should be discussed to develop habits of 'acceptable use'; that can then be applied to other social networking platforms. In particular pupils will recognise that some families and children may not wish to communicate via Blick!. Permission to use this facility will be withdrawn if there is a serious breach of the acceptable use policy.
- Pupils in years 5/6 will be taught specifically about social networking sites.
- All access to social networking sites will follow the acceptable use guidance.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and risk. This will be considered before use in school is allowed.

Protecting personal data, publishing child's images and work on the school website and newsletter

- Personal data will be recorded, processed, transferred and made available according to the UK GDPR - General Data Protection Regulation.
- The school will maintain an up-to-date GDPR register of individual GDPR preferences for each child.
- The school will appoint a member of staff with overall responsibility to comply with the GDPR permissions. The current post holder is Lucie Hunter.
- Photographs that include pupils will only be allowed to appear on-line (i.e. the school website) in line with individual GDPR permissions.

- A child's full name will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Child image **file names** will not refer to the child by name.
- Parents should be clearly informed of the school policy on image taking and publishing, this information appears on the Registration Form and the GDPR consent form.

Authorising Internet access

- All school staff and pupils are granted access to school ICT systems and school internet on the basis they will follow this policy and the accompanying ICT Acceptable Use Policy. Permission to use the school ICT system may be withdrawn when there has been a serious breach of the acceptable use policy, misuse of the ICT system, internet or ICT equipment.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- The school will regularly assess the e-safety policy and procedures to ensure they are adequate and remain appropriate.

Handling e-safety complaints

- Any e-safety concerns can be directed to the Principal.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school Safeguarding and Child Protection procedures.
- Children and parents will be informed of the complaints procedure where appropriate.
- Children and parents will be informed of consequences for children misusing the Internet.

Pupils and the e-Safety Policy

- E-Safety rules will be regularly referred to in all year groups as appropriate and as the need arises.
- E-Safety training is embedded within the ICT curriculum and Personal Social Health and Economic curriculum(PSHE). It is also included in the school's commitment to the ***Prevent*** strategy.

Staff and the e-Safety Policy

- All staff will be given the School e-Safety and acceptable use Policy and its importance explained.

Parents' and carers' and the e-Safety policy

Parents and carers attention will be drawn regularly to the School e-Safety Policy in newsletters, the parents' information book and on the school Web site. Parents talk/training in e-safety will be scheduled in the programme of talks for parents.

2. ICT ACCEPTABLE USE POLICY

Annan School provides a range of ICT resources which are available to all staff and pupils. In order to ensure the safety of both staff and pupils, it is important that all users follow the guidelines detailed below.

Terms of Acceptable Use

This policy applies to all staff and pupils at the school, regardless of their use of ICT systems.

Internet Access

The school provides internet access for all staff and pupils in order to allow access to the wide range of content available.

- It is not permitted to attempt to access, on any device, inappropriate, illegal, offensive or discriminatory websites or to access (or download) any racist, radicalised or extremist material in school or on any school-owned equipment such as laptops, wherever these are used.
- On-line school communication must be made through the school's **MS Teams platform**, by using the username and password issued to all staff and pupils at the school. Staff and pupils should not log-in as another member of staff or pupil.
- No pupil or member of staff may download any software from the internet for installation onto a school computer system.

Personal use of School Equipment

- The ICT equipment provided by the school is for work relating to the school only.
- No personal applications, mail accounts or personal photographs should loaded onto any school computers, laptops or cameras.
- Staff only: when accessing files, photographs or other school related data, when not on the school premises, staff should be mindful that this cannot be viewed by other people or family members. Staff should log-out of programmes and/or the laptop/camera when leaving it unattended.

Digital cameras

The school encourages the use of digital cameras and video equipment, however all users should be aware of the following guidelines **with particular reference to the EYFS**

- **See Appendix 2 - Camera, Photograph and Social Networking Guidance** (at the end of this Policy)
- Digital cameras or mobiles with cameras are provided by the school for use by school staff and pupils.
- Personal digital cameras or cameras on mobile phones may not be used by pupils or members of staff.

Applies to staff only:

- All photos should be uploaded to the School Dropbox account. Any queries regarding this should be referred to Lucie Hunter who has overall responsibility for the photographs retained by the school.
- When using printed versions of the photographs, these should only be named with the child's name if they are to be accessible in school only (i.e. for Learning Journeys).

Personal Mobile Phones (pupils)

- Pupils may not bring a mobile phone or any other electronic device into school. For exceptions see **APPENDIX 1 - Mobile Phone Use Guidance**

Personal Mobile Phones (staff)

Personal mobile phones are permitted under the following guidelines:

- **See APPENDIX 1 - Mobile Phone Use Guidance for Staff Including the EYFS**
- **Personal Mobile Phones** must not be used when staff are directly supervising or working with pupils.
- Personal mobile phones may be taken **for emergency contact** on outings and at forest school.
- Mobile phone **cameras** are not to be used on the school site, or any school outings. The school provides cameras for this purpose (see *Digital Cameras* above).
- All phone contact with parents regarding school issues will be through the **school's phones** (except in the case of peripatetic music teachers etc)
- Staff must not give their personal phone number to parents unless absolutely necessary (for example an exception might be the minibus driver regarding a pick-up).
- Under no circumstances should a member of staff give their mobile phone number to a pupil at the school.

School Computer Network Security

- Pupils are not allowed to use a computer/laptop which is logged on to the Staff area of the network;
- Pupils are not allowed to use **personal** laptops belonging to a member of staff;
- When any computer, laptop or camera is left unattended, it should usually be logged off or locked.
- Pupils and staff should not use a computer which is found logged on, it must be logged off, and re-logged in as necessary.

  Staff only:

- Each member of teaching and support staff is allocated a staff password to access the Pupil and Staff portals on the School Teams channels and AIMS (School Information system). Staff are responsible for ensuring the password remains confidential. If staff forget their password or believe someone else knows their password they should contact Lucie Hunter for a new password. Staff will only access areas which they have been authorised access.

File Storage

- Each class has their own personal file storage area on the Teams Portal (Blick!) for their class, as well as access to shared files on Blick!. Any school related work should be stored in Teams and not on individual laptops. Personal files are not permitted on the network areas or on laptops belonging to the school.
  In addition staff have storage areas for school related files on the Teams Portal (School Team).
- Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files.
- Staff and pupils must not transfer or copy school related files to removable data sticks or other key-drives.
- Staff and pupils are permitted to access the MS Teams Portal (Blick or School Team) on a personal laptop, PC or mobile phone, away from the school site, provided this is logged in directly via the MS Teams website or MS Teams App. No school data is to be downloaded to a personal computer belonging to a member of staff or pupil. The above security protocol for logging-out etc., when using school equipment should also be followed when using personal laptops.

Social networking

- For the purposes of this section the term 'friends' is used to define any link created between the online profiles of 2 or more people.
- Under no circumstances are staff permitted to be 'friends' with any pupil of the School who is not a direct relative.
- The School recommends that staff are not 'friends' with any ex-pupil of the school who is under the age of 18.
- The School recommends that staff are not 'friends' with other parents of the school unless a relative or very close friend.
- No details or opinions relating to any child or member of staff are to be published on any website or social media.
- No communication should take place between parents (or pupils) and staff members regarding any issues relating to the school, staff or pupils using publicly accessible social networking sites.
- No photos or videos which show children of the school who are not directly related to the person posting them should be uploaded to any site or on social media (ie Facebook or Twitter).
- No comment, images or other material may be posted anywhere, by any method that may bring the school or the profession into disrepute.

Policy monitoring and review

This policy, and accompanying Appendices, is monitored by the Principal and staff of the school and will be reviewed annually.

APPENDIX 1

MOBILE PHONE USE GUIDANCE FOR STAFF (including use of mobile phones by pupils)

Aim

The aim of the mobile phone guidance is to protect pupils from harm, by ensuring the appropriate management and use of mobile phones by all individuals who come into contact with pupils at the setting.

Scope

This guidance relates to the use of mobile phones for calls and texts. The use of mobiles with camera capability is covered in the separate camera guidance *(Appendix 2)*. This guidance covers children, parents and carers, teachers, TA's, and support staff and includes volunteers, students, visitors, contractors and peripatetic teachers and anyone else in the school buildings and grounds or accompanying children during off-site activities. This guidance should be read in conjunction with the school's *Camera, Photograph and Social Networking Guidance. (Appendix 2)*

Use of mobile phones by staff

All personal mobile phones belonging to staff will be stored in staff lockers or where staff keep coats and bags. Mobile phones must be turned off or switched to silent during contact time. Staff may only check their messages when they have non-contact time. Staff may use the staff areas or classrooms outside of lesson time. In exceptional circumstances if a member of staff must be contactable for personal reasons they must obtain permission from the Principal to carry their phone with them and then leave the classroom to take the call having made arrangements for the supervision of any pupils in their care. Staff should give the school landline as their first emergency contact when they are working.

Mobile phones for emergency contact when away from the school site

When groups of pupils leave the school site – ie forest school, wildlife area, outings, the teacher in charge should ensure they have a charged and working mobile phone for emergency contact.

Staff should not use their own personal mobile phones for contacting children and parents and carers and should not give parents their personal phone numbers.

Use of mobile phones by other adults

Mobiles should only be used in areas not in use by pupils. Anyone helping with supervision of pupils on school outings or within school must be made aware that they should not use their phone whilst in charge of a group of pupils. Other adults such as parents, visitors, students etc who receive a call or need to make a call, read or send messages must do so in the car park and not in any teaching or cloakroom areas.

Use of mobile phones by pupils

Pupils may not bring a mobile phone or any other electronic device into school. The only exception to this is when a child uses the minibus and parents may need to contact them in relation to arrangements regarding collection from the minibus. This exception must be agreed between the parent and the school. Pupils are not allowed to have access to their phone during the school day. Phones should be handed in at the school office and pupils are responsible for collecting the phone at the end of the school day. It may then only be used when the child reaches their drop-off point. It must not be used whilst travelling on the minibus. Any breech of such conditions will mean that parents will be informed and future permission to have a phone in school may be withdrawn. The school cannot accept responsibility for loss or damage.

Mobile phone use while driving

Under no circumstances, when driving on behalf of the school, should staff or parents make or take a phone call, text or other functions of a mobile phone. This also applies to the use of hands free and wireless connections unless in an emergency.

APPENDIX 2

CAMERA, PHOTOGRAPH AND SOCIAL NETWORKING GUIDANCE

Aim

The camera, photograph, and social networking guidance aims to ensure safe and appropriate use of cameras and storage of images through agreed procedures.

Scope

The camera, photograph, and social networking guidance applies to children, parents and carers, teachers, teaching assistants, volunteers, students, visitors, and contractors.
The camera and photograph guidance applies to the use of any photographic equipment.
This includes mobile phones and portable gaming devices with inbuilt cameras as well as other forms of digital technology and resources for storing and printing images.

This guidance should be read in conjunction with the school's *Mobile Phone Use Guidance.*

Responsibilities

The Principal is responsible for ensuring the acceptable, safe use and storage of all school camera technology and images. This includes the management, implementation, monitoring and review of the camera, photograph, and social networking guidance. Consent for the use of images for publicity materials, or to support the training needs of teaching staff etc., is sought from parents when their child registers at the school. The Principal may delegate this responsibility to a person appointed for that role. The current post holder is Lucie Hunter.

Acceptable use of photographs/recordings

Staff regularly take photographs of the pupils to record their activities and achievements, and these can be put in their individual learning journeys. They are also displayed around school. Photographs are also used on the website, newsletters and other publicity materials. All photographs should be taken using a school camera. Staff and other visitors are not permitted to take photographs using personal cameras or mobile phones unless explicit permission has been given by the Principal.

Staff should not take photographs if a child refuses permission or appears uncomfortable about having their photograph taken. Cameras must never be used in areas where pupils are using the toilet or undressed. Photographs should not be taken which may cause distress, upset or embarrassment.

Photographs may only be stored on the school network, temporarily on school camera SD cards or the built-in memory on the school iPhones cameras.

The main photo library is on Dropbox where images are stored. Access to this is restricted to teaching staff and is password protected.

Parents and carers/visitors taking photographs or recordings

At open events (i.e. events which parents and visitors are invited to attend) parents/carers may take photographs or make recordings for their own personal use unless instructed otherwise by the Principal or other member of the school staff. At other times when general permission has not been given they must ask permission of the teacher in charge at the time (such as inside a teaching area when a parent has been invited to look at their child's work). However, **parents assisting with activities both in school and on educational visits away from school are not permitted to take any photographs on personal devices**.

Visitors to the school, including students and visiting practitioners, will only be permitted to take photographs of the school buildings/equipment on those occasions when no children are present, provided prior consent has been sought. When photographing children's work the names of children should not accompany the photograph, and photographing work or displays where children can be identified is not permitted.

Pupils photographing each other – use of school and personal cameras

- Pupils may be given the opportunity to photograph each other and their surroundings to support their learning and development needs. Such photographs must be taken on school cameras. Teachers should discuss and agree acceptable use rules with pupils regarding the appropriate use of school cameras. These should include asking permission before taking photographs of other pupils or members of staff, and not taking inappropriate photographs which may cause distress, upset or embarrassment.
- Children may request to bring a personal camera on an educational visit or activity. In these circumstances the teacher will need to give permission and set 'acceptable use' rules. When using personal cameras, pupils may not photograph other pupils or staff (including group photographs).

  Exception to this may be made, for example on the year 5/6 residential, but only with permission of the teacher in charge and agreement of the children who may appear in the photographs, and in line with the permissions given by parents as part of GDPR.

Use of images of pupils by the media

- There may be occasions where the press are invited to a planned event to take photographs of the pupils. It should be noted that the press enjoy special rights under GDPR, which permit them to publish material for journalistic purposes.
- Parents will be informed if the Press are to take photographs and given the opportunity to ask that their child is not photographed.

Other procedures

Electronic images will be protectively stored and password protected within the school's photographic storage system (currently Dropbox). Images will not be kept for longer than is to be considered necessary. Photographs will be deleted from memory cards, portable drives or other relevant devices once the images have been uploaded or is no longer of use. Such equipment will be stored securely and access is restricted.

Professional portrait photographers

Only recognised photographic companies or photographers are used. Parents are asked in advance if they wish to withdraw permission for their child to be photographed. Photographers are not given unsupervised access to the pupils. Pupils are accompanied by a member of staff when photographs are being taken. Photographers give their agreement that all images taken are for use by the school and for no other purpose.

Social networking sites

Staff Usage

Staff must follow the Policy regarding Social Networking contained in the school's ICT Acceptable Use Policy

- Work related postings between staff should be contained within the MS Teams (School Team)
- Staff should ensure that they have set up maximum privacy settings on social networking sites they use.
- All communications and postings on social networking sites should be of a personal nature and not work related.
- Staff should have regard to the professionalism of their position and avoid postings which could compromise this.

Parent Usage

- Parents should not attempt to make contact with staff at the school through social media.
- Any photographs or recordings taken by parents at school events, which have other people's children in them, should not be uploaded to social networking sites.
- Parents also need to ensure that they protect the reputation of the school in any postings they may personally make.