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 is 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*

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

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

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 children 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 children.

Internet use will enhance learning

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

Children will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and children complies with copyright law.
- Children will be taught the importance of cross-checking information before accepting its accuracy.
- Children 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 PSHE and sex and relationships education. It is also included in the school's commitment to the ***Prevent*** strategy.
- Children will take part in discrete safety lessons appropriate to the age of the children.

MANAGING INTERNET ACCESS AND SAFETY

Internet safety

- We take a 'whole school approach to on-line safety'.
- The school will ensure appropriate filters are in place to safeguard children from potentially harmful and inappropriate material on-line, but without an unreasonable level of blocking.
- The school will consider its duty in response to the ***Prevent*** strategy to make appropriate provision to prevent children being influenced or targeted to participate in radicalism or extremism.
- Children are not allowed access to personal 3G & 4G enabled devices on school premises, or during school activities, unless by agreement with the Principal (ie in the case of SEND or EAL) in which circumstances 3G & 4G safety will be considered on a case by case basis
- 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.

E-mail

- Email use must follow the guidance of the staff Acceptable use agreements (see below)

Publishing child's images and work on the school website

- Photographs that include children will be selected carefully and will only be allowed to appear on-line (ie the school website) with the approval of the Principal.
- Children full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Photographs in which an individual child can be identified will not be published on the school website if this goes against the wishes of parents/guardians or the child.
- 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.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate children in their safe use.
- Children 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

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

POLICY DECISIONS

Authorising Internet access

- All school staff and children are granted access to school ICT systems and will follow the acceptable use guidance.

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

Children 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, Personal Social and Health Education (PSHE) curriculum and sex and relationships education. 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. In order to ensure the safety of both staff and children, it is important that all staff follow the guidelines detailed below.

Terms of Acceptable Use

This policy applies to all staff of the school, regardless of their use of ICT systems

School Email

- All teaching staff are provided with a school email address. The email system can be accessed from both the school computers, and via the internet from any pc.
- The sending of emails is subject to the following rules:
    - Language must not include swear words, or be offensive or abusive.
    - Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted. This includes attempts to encourage or promote participation in **radicalism or extremism,** or give views of a one-sided political nature.
    - Sending of attachments which contain copyright material to which the school does not have distribution rights is not permitted.
- Staff are not permitted to send emails to parents using personal email addresses, unless agreed by the Principal (for example peripatetic music staff)
- All staff should be aware that email is not a secure communications medium, and therefore should not be used for the transition of confidential files or staff / student data.
- Staff are not permitted to send via email any information which is covered by the Data Protection Act, without prior written authorisation from the schools data protection officer (Mark Hunter).

Internet Access

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

- It is not permitted to attempt to access, on any device, pornographic, illegal, sexist, violent, racist, radicalised or extremist material in school.
- The use of online real-time chat rooms is banned, unless specific permission is sought from the Principal.
- No member of staff may download any software from the internet for installation onto a school computer system without prior authorisation from the Principal.

Personal use of Equipment

The ICT equipment provided by the school is for work relating to the School. Should a member of staff need to use any ICT equipment for personal use this could be permitted provided that:

- The member of staff has sought permission from the Principal.
- Any activities carried out on them complies with the other terms of this policy.
- No personal applications are loaded onto any computers/laptops.
- No technical support is provided by the school for problems arising as a result of personal work on the equipment.

Digital cameras

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

- See: **Appendix 2 - Camera, Photograph and Social Networking Guidance**

In addition:

- Photos should only be named with the child's name if they are to be accessible in school only – photos for the website or other media must only include the child's first name.
- Digital cameras are provided by the school for use by school staff and children. With the permission of the Principal, personal digital cameras may be permitted, except those which are integrated into mobile phones. However images of children must be downloaded to the school network and removed from the camera before it leaves the school site.
- All photos should be downloaded to the school network.
- The use of mobile phones for taking photos of children is not permitted.

Personal Mobile Phones (staff)

Personal mobile phones are permitted within the boundaries set under the following guidelines:

- See: **APPENDIX 1 - Mobile Phone Use Guidance for Staff Including the EYFS**

In addition:

- **Personal Mobile Phones** must not be used when staff are directly supervising or working with children.
- 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 digital 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)

School Computer Network Security

- Each member of teaching and support staff is allocated a staff password to access the Pupil and Staff areas of the school network. Staff are responsible for ensuring the password remains a secret. Staff will only access areas which they have been authorised access;
- Children should not be allowed to use a computer which is logged on to the Staff area of the network;
- Children should not be allowed to use personal laptops belonging to a member of staff;
- When any pc is left unattended, it should usually be logged off or locked. Staff should not use a computer which is found logged on, it must be logged off, and re-logged in as necessary.

File Storage

- Each class teacher has their own personal area on the network for their class, as well as access to shared files on the network drive. Any school related work should be stored on one of these areas and not on individual laptops. Personal files are not permitted on the network areas or on laptops belonging to the school.
- Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files.
- Any files stored on removable media must be stored in accordance with the following policy:

  No school data (relating to individual children) is to be stored on a personal computer belonging to a member of staff, or un-encrypted storage device. Staff are permitted to work on such files on a personal computer (i.e. preparing reports) with material accessed via an encrypted storage device (memory stick), provided that such data is transferred to the school network for storage as soon as possible and, once transferred, deleted from storage/transfer media.

Social networking

The key requirements for staff are as follows:

- 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 child of the School who is not a direct relative.
- The School recommends that staff are not 'friends' with any ex child 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 are to be published on any website or social media.
- No opinions regarding another member of staff which could cause offence are to be posted.
- No communication should take place between parents (or children) and staff members regarding any issues relating to the school or children 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), unless with the specific agreement of the Principals.
- No comment, images or other material may be posted anywhere, by any method that may bring the school or the profession into disrepute.

APPENDIX 1

MOBILE PHONE USE GUIDANCE FOR STAFF INCLUDING STAFF IN THE EYFS

Aim

The aim of the mobile phone guidance is to protect children from harm, by ensuring the appropriate management and use of mobile phones by all individuals who come into contact with children at the setting. Mobile phones can also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others.

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. The 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.*

Use of mobile phones by staff

All personal mobile phones belonging to staff will be stored in staff bags 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 children in their care. Staff should give the school landline as their first emergency contact when they are working. Mobile phones cannot be relied on as a time piece and staff should ensure they have a wrist watch.

Mobile phones for emergency contact when away from the school site

When groups of children leave the school site – i.e. forest school, sports field, outings, the teacher in charge should ensure they have a charged and working mobile phone for emergency contact. If the phone is not the one listed as belonging to the teacher in charge, they should ensure the mobile number is given to the office in case the school needs to contact the group in an emergency.

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 children. Anyone helping with supervision of children on school outings or within school must be made aware that they should not use their phone whilst in charge of a group of children. 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 children

Permission for children to have a phone at school is at the discretion of the class teacher. Children are not allowed to have access to their phone during the school day unless supervised by a member of staff. Any breech of such conditions will mean that parents will be informed and future permission to have a phone in school may be withdrawn. Parents who wish their children to have a mobile phone in school agree that 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.

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.

Acceptable use of photographs/recordings

Staff regularly take photographs of the children to record the children's 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. It should be ensured that a child's full name does not appear in any caption or accompanying text alongside their photograph, for example on displays, documentation panels and name cards. Cameras must never be used when children are using the toilet or undressed.

Staff should not take photographs if a child looks uncomfortable in any way or refuses permission. Photographs should not be taken which may cause distress, upset or embarrassment.

Photographs may only be stored on the school network or temporarily on school USB sticks/camera SD cards. Access to the network where images are stored is restricted to teaching staff and is password protected.

Parents and carers/visitors taking photographs or recordings

At open events (ie events which parents and visitors are invited to attend) parents and 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 or when taking photographs of children other than their own).

With permission, visitors to the school will only be allowed to take photographs of the school buildings/equipment avoiding clear images of children and names of children will not be given to identify any children in the background.

When acting in a supervisory role such as on outings, parents are not permitted to take photographs using *personal* cameras or mobile phones.

Children photographing each other

Children may be given the opportunity to photograph each other and their surroundings to support their learning and development needs. Teachers should discuss and agree acceptable use rules with children regarding the appropriate use of cameras. These should include not taking inappropriate images and keeping images for their own use only. The same usage rules will apply if children bring their own personal cameras to school or on a school trip.

Use of images of children by the media

There may be occasions where the press are invited to a planned event to take photographs of the children. It should be noted that the press enjoy special rights under the Data Protection Act, 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

All images, including those held within learning journeys will remain on site at all times, unless consent has been given by the Principal. Images must be protectively stored and password protected on the computer hard drive or other appropriate storage device as far as possible. Images will not be kept for longer than is to be considered necessary. Photographs should be wiped from memory cards, computer hard and portable drives or other relevant devices once the images are 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 children. Children 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 should ensure that they have set up maximum privacy settings on any social networking sites they use.
- All communications and postings on social networking sites should be of a personal nature and not work related.
- Work related postings between staff should be contained within the school staff Facebook group.
- 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 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.