

FRIENDS' SCHOOL LISBURN

Preparatory Department



E-Safety Policy

Contents:

1. Aims
2. Roles and Responsibilities
3. School Systems
4. Pupils
5. Cyberbullying
6. Staff
7. Parents
8. Use of Digital Images
9. Infringements of the E-Safety Policy
10. Appendices
 - i. AUP for pupils
 - ii. AUP for Staff
 - iii. Data Security Policy

1. Aims

The aims of the policy are to ensure that:

- digital and online technologies are used safely to enhance teaching and learning in School;
- ICT and facilities provided by School are used in a manner in keeping with the values and aims of Friends' School.

2. Roles and Responsibilities

Governors have responsibility for approving and reviewing the E-Safety Policy, and the Principal and the Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Leadership Team has responsibility for:

- providing training and advice for all staff
- liaising with school technical staff
- receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments
- reporting regularly to the Principal and Governors

The Designated Teachers for Safeguarding and other staff with particular pastoral responsibilities, including Teachers, are trained in e-safety issues and are aware of the potential for serious child protection and safeguarding issues arising from:

- sharing of personal data
- access to illegal or inappropriate materials
- inappropriate on-line contact with adults
- potential or actual incidents of grooming
- cyber-bullying

3. School Systems

The School uses a Managed System, maintained by C2k/ Capita, and will ensure that:

- All equipment is maintained safely and access is restricted to those who require it
- All users are provided with a username and secure password and are responsible for their security.
- Internet access is filtered, with differentiated filtering levels for different groups of users
- The use of C2k services, including C2k email and the C2k VLE (Fronter), is encouraged, in line with School policy
- The Head of Department or Systems Manager provides temporary access for guests (such as trainee teachers, supply teachers and visitors) on the school systems.
- An agreed policy is in place regarding personal use that users and their family members are allowed on school systems and school devices used outside school (Appendix 2)
- Personal data is not to be sent over the internet or taken off the school site unless safely encrypted or otherwise secured; further information on this can be found in the policy on Data Protection (Appendix 3)

4. Pupils

Education in e-safety is an essential part of the School's provision, allowing pupils to recognise and avoid e-safety risks and to build their resilience. The following measures are in place to educate pupils in e-safety:

- Pupils are given specific guidance in safe and acceptable online behaviour through the discrete ICT classes and through Anti-bullying and Personal Responsibility lessons taught as part of the PDMU

- Key e-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities.
- Staff are supported in this by external agencies such as the PSNI, who are invited into school to address pupils about issues surrounding e-safety
- E-safety is highlighted in School Planners to raise awareness of this issue with pupils and parents.
- E-safety is referenced in Schemes of Work in all areas of the curriculum

The School operates a policy which does not allow pupils to use mobile devices within school.

5. Cyberbullying

Offensive material relating to School, or any member of the School community, should not be posted on the internet, regardless of whether this has been done at school or in any other place, including a pupil's home.

- All instances of cyberbullying – online behaviour which seeks to harass, intimidate or humiliate others – is forbidden and will be dealt with according to the school's Anti-Bullying policy.
- If pupils think they are being bullied online, they should speak to a member of staff as soon as possible.
- If Staff feel that they are abused online, they should speak to the Head of Department as soon as possible.

6. Staff

Staff are encouraged to act as good role models in their use of digital technologies, the internet and mobile devices, and to abide by the guidelines set out in Appendix 3. To ensure that staff are aware of issues surrounding e-safety:

- E-safety forms part of annual staff training on Safeguarding
- E-safety is part of the planned programme of CPD for all staff, including non-teaching staff

7. Parents

Parents and carers have a responsibility for ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school helps parents understand these issues and encourages parents and carers to support the school in promoting good e-safety practice by:

- Providing information through School Planners and Parentmail about e-safety issues
- Providing opportunities for parents to come into school to attend talks on e-safety

8. Use of digital and video images

Staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet, and the associated problem of cyberbullying. It is difficult to remove digital images from the internet permanently and they can cause harm or embarrassment to individuals.

When using digital images, staff should inform and educate pupils about the risks associated with taking, sharing, publishing and distributing images. In particular, they should recognise the risks attached to publishing their own images on the internet, including on social networking sites.

The following measures are taken to ensure that correct procedures are in place in relation to digital images:

- Parents of new pupils entering School are asked to give their written permission for images to be taken for publicity purposes (in displays, on the school website and plasma screen and in the press) and for a pupil photograph to be stored on the C2k system.
- Parents may 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. However, to respect everyone's privacy and protection, these images should not be made publicly available on social networking sites.
- Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere, will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupil work will only be published with the permission of the pupil and parents.

The Bursar is responsible for the operation of CCTV which is used to monitor certain areas of the School premises. Appropriate signage indicates the presence of CCTV cameras at all locations and no additional cameras should be installed by anyone anywhere on the School premises. Images taken by CCTV cameras are stored and may be reviewed if necessary.

9. Infringements of the e-safety policy

When infringements of the policy take place, through careless, irresponsible or deliberate misuse of school systems or devices, incidents will be dealt with as soon as possible and will be handled in a proportionate manner, in line with other school policies, including the anti-bullying policy.

In the case of more serious infringements, the following procedure will be followed:

- at least two members of staff will be involved in the investigation
- clear records will be kept of the investigation, including details of sites and content visited
- URLs and screenshots may be recorded for investigation, except in the case of images of child sexual abuse, where the matter will be referred immediately to the police
- the computer in question will be isolated, as any change to its state may hinder a later police investigation.

If there is reason to believe that illegal activity has occurred using school systems or school devices, the matter will be passed on to the police

Monitoring and review

This policy will be reviewed in the light of technological advances and changes in the equipment available in school.

Staff will be asked to share examples of good practice with colleagues; this will inform how the policy evolves. Pupils and parents are also encouraged to share ideas with staff about how information technology, including individually owned electronic devices, can be used to enhance teaching and learning safely.

Appendix 1: Friends' School Lisburn Acceptable Use of ICT Policy for Pupils

This AUP should be read in the broader context of the School e-safety policy and has two main aims:

1. to enhance learning by allowing pupils at Friends' Preparatory Department the freedom to use School ICT facilities as a tool to help them in their learning.
2. to protect the school community from the negative aspects of the use of ICT.

C2k Managed Service

- A filtered internet and email service is provided in School through C2k. All pupils are provided with an email address and password. Pupils are encouraged to use this facility to: research, create, store and print material related to the curriculum
- communicate with other pupils, members of staff, recognised outside agencies and pupils in partner schools
- support their learning through the VLE (Fronter)

Pupils should know and understand that no user of School services is permitted to:

- use another user's password or user name
- introduce unauthorised software to the system
- cause damage to equipment

Pupils are advised that School has the ability to review files and communications, and to monitor work remotely, to ensure that everyone is using the system responsibly.

Use of the internet

Access to the internet in school should be exclusively through the C2k network. It is School policy to promote the use of C2k services, including C2k email and the C2k VLE (Fronter). Pupils should not use the mobile phone network to access the internet unless they have permission from a member of staff to do so. Pupils using devices with internet capability should only access the internet through their MY-SCHOOL page and should be aware that downloading data may incur a cost.

The following online activities are not permitted:

- the use of social networking, file sharing or gaming sites, unless permission has been given by a member of staff in relation to a classroom activity
- unfair usage (for example, downloading or uploading large files, thereby hindering others in their use of the internet).

Recording and storage of sound and images

The recording and storage of sound, or of still or moving images is allowed only with the permission a member of staff. If images are recorded, this will be done in accordance with the School's policy on the use of photography.

Photographs, sound files or videos produced in School should not be posted on the internet unless there are special circumstances in which permission to do so has been granted. Pupils must allow staff access to images and sound files created in school, including those stored on personally owned electronic devices, and must delete them if requested to do so.

Cyberbullying

Offensive material relating to School, members of staff or other pupils should not be posted on the internet, regardless of whether this has been done at school or in any other place, including a pupil's home. All instances of cyberbullying – online behaviour which seeks to harass, intimidate or humiliate others – is strictly forbidden and will be dealt with in line with the school's Anti-Bullying policy. If pupils think they are being bullied online, they should speak to a member of staff as soon as possible.

Additional notes on the use of mobile electronic devices

Use by Pupils:

- Pupils should only have mobile phones in school if they are needed to contact parents after school hours.
- The phone should be switched off, handed in and placed in the class teacher's desk during the school day.
- Parents must inform the appropriate class teacher, in writing, at the beginning of each school year, if their child needs to bring a mobile phone to school. Should the need arise during the course of the school year for a pupil to bring a phone to school on any occasion, the class teacher must be informed in writing.
- If a child needs to contact a parent or if a parent needs to contact a child during school hours, this should be done via the school secretary.
- Use of electronic devices in class is entirely at the discretion of teaching staff. Pupils should follow the instructions of their teachers and should not access any websites, apps or programs other than those required for the completion of the task set.
- The School does not accept responsibility for the theft or loss of devices, or damage to them. Pupils are also responsible for all software and applications installed on personal electronic devices. The School cannot accept any responsibility for problems associated with software and apps pupils installed on devices. Pupils should ensure that their devices are properly protected by suitable anti-virus software at all times.

Use by Staff:

- During the day mobile phones must remain in handbags/drawer of desk and on silent when teachers are in their classrooms or at After School Club.
- Mobile phones must not be used in the playground, in the classroom or in the corridors when children are present.
- If a member of staff is awaiting an important call he/she should inform the Head of Department that his/her phone may ring in the classroom or at After School Club. Pupils should also be made aware that this may happen and if appropriate, the exceptional circumstances for the teacher or staff member having to take the call.

Sanctions

If a pupil is found to be in breach of any aspect of this protocol, the School reserves the right to confiscate a pupil's electronic device, or to withdraw permission, either temporarily or permanently, for the pupil to bring the device into School. Should a device be confiscated, a pro forma will be filled in, giving details of the reasons for confiscation and recording the condition of the device confiscated.

The device may then be collected by a parent from the office at the end of the school day. Additional action may be taken in line with existing policies on Anti-Bullying and Behaviour for Learning. If there are reasonable grounds to believe that a pupil's electronic device contains images, text messages or other material that may constitute evidence of criminal activity, the School reserves the right to pass devices on to the police for further investigation.

Appendix 2: Friends' School Lisburn Acceptable Use of ICT Policy for Staff

E-Safety

Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school e-Safety Policy and practices
- they have read, understood and signed this Acceptable Use Policy
- they report any suspected misuse or problem
- all digital communications with pupils and parents are on a professional level and are only carried out using official school systems.

In addition, all staff share responsibility for ensuring that:

- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- pupils are aware of their 'digital footprint' and how this can affect them
- they monitor the use of digital technologies and mobile devices, including phones, tablets, MP3 players and cameras, in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils are 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
- settings on computers and mobile devices are secure so that no sensitive or personal information, including passwords and emails, are displayed on screens in classrooms

Communications

When using communication technologies the school considers the following as good practice:

- The official C2k email service should be used where possible as it be regarded as safe and secure, and is monitored.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, or is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents must be professional in tone and content.
- Pupils should be taught about e-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

School staff should ensure that:

- Due care is taken when reference is made on social media to pupils, parents or colleagues
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions are not attributed to the school
- Security settings on personal social media profiles are regularly checked.

Digital Images

Staff and volunteers may take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Images should not be stored any longer than is necessary on personally owned devices

- Care should be taken when taking digital or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Mobile electronic devices (including mobile phones)

- Staff should not send texts or make private phone calls during class time.
- Personal calls and texts should not be received in class time except in exceptional circumstances
- Staff are asked to use their discretion when using mobile devices on the school premises
- Digital images should not be stored on personal mobile devices
- Communication with pupils and parents should be restricted to School business, and staff are advised to use school telephones, C2k email or Parentmail to communicate with pupils and parents.
- Staff who have been issued with mobile electronic devices by School (including iPads) should ensure that these are used primarily for School purposes, and that access to them is restricted so that confidential information is not viewed by others.
- School reserves the right to recall and redeploy devices in order to maximise the benefit of these devices in teaching and learning.

Appropriate use of ICT

Staff are encouraged to use ICT to enhance teaching and learning and it is recognised that it can be useful in many different contexts, including on school trips and at events organised by School. However, in the interests of their own safety and that of others, all staff should be aware of what constitutes appropriate professional conduct in matters relating to e-safety.

Care should be taken when using sites dedicated to online shopping, online gaming, file sharing and social media. In addition, the following activities are deemed unacceptable and may in some cases constitute illegal behaviour. They should not therefore be carried out in school or using school owned devices:

- Unfair usage (for example, downloading or uploading large files, thereby hindering others in their use of the internet)
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Using school systems or devices to run a private business
- Infringing copyright
- The publication of information which may be offensive to colleagues or breaches the integrity of the ethos of the school, or brings the school into disrepute