Friends' School Lisburn

E-Safety Policy

Contents:

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 and the School E-safety Officer have 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 Leadership Team and Governors

The Designated Teachers for Safeguarding and other staff with particular pastoral repsonsibilities, including Year 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 Vice Principal 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 Year 8 and 9 ICT classes and through Anti-bullying and Personal Responsibility modules taught as part of the KS3 LLW curriculum
- Key e-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities and through elements of the Pastoral Calendar, delivered by Collect Staff.
- 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 allows pupils in the Sixth Form to bring mobile devices into school. Pupils are asked to sign an AUP agreeing to the terms of the BYOD policy before being allowed access to the school network (see Appendix 2)

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 a member of the Leadership Team 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.