Baginton Fields School

Policy for E-Safety

“Working together for outstanding achievement”

Review: Spring 2022

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone and are an essential element in 21st century life for education. As part of their learning experience the school has a duty to provide pupils with quality Internet access along with an understanding of how to safely use other information technologies.

The purpose of ICT and internet use at Baginton Fields School is to:

- Raise standards, promote student engagement and achievement
- Support the professional work and development of staff
- Enhance the school's management information and administration systems

Children and young people should always have an entitlement to safe internet access.

The requirement to ensure that children and young people can use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work at Baginton Fields School are bound. The school E-Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, and the students themselves. E-safety is taught as part of the school curriculum and is part of the school assessment tool. (See IT and Computing Curriculum Policy)

The resources used by students in school are carefully chosen by the teacher and determined by our curriculum. However, use of the internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst students will often be directed to sites which provide reviewed and evaluated sources, they may move beyond these (through choice or accidentally), to sites unfamiliar to the teacher. There is therefore a genuine cause for concern and a need to raise awareness in order to promote the highest possible levels of safeguarding. This policy has been developed in order to allow staff, parents, carers and students to have an awareness of internet safety issues, and some guidelines for the safe and responsible use of the internet. The procedures and guidelines within it aim to balance the obvious benefits and educational potential of internet use, whilst providing safeguards against the risks.

Risks

- Copyright infringement
- Obsessive use of the internet and ICT
- Exposure to inappropriate materials
- Inappropriate, antisocial or illegal behaviour
- Physical danger and abuse
- "Cyberbullying"
- Inappropriate use of social networking media

With these risks in mind, students at Baginton Fields will:

- Have the school's E-safety rules explained
- Be supervised appropriately
- Be given clear objectives for internet use
- Be educated in responsible and effective internet use (IT and Computing Curriculum Policy)

Control Measures

The following measures have been adopted to help ensure that students are not exposed to unsuitable materials:

- The school network is connected to Coventry City Council's "firewall" to prevent unwanted network use, and a filtering system to prevent access to inappropriate material
- Staff will check that sites pre-selected for use are appropriately screened in order to ensure suitability
- Staff will supervise internet use appropriately and be particularly vigilant when allowing students to undertake their own searches
- Students will be taught to use the internet and email responsibly and safely
- Students may use email as part of planned lessons. In this instance, outgoing messages will be checked by staff members. Any in-coming messages will not be regarded as private and will be screened by staff.
- Students will be taught about the potential risks of email attachments
- The school will employ anti-virus and anti-phishing control measures
- Rules for responsible internet use will be on display
- Forensic software such as Imperio is used to monitor internet usage and report inappropriate usage to the technicians, Headteacher and Safeguarding lead.
- A record of any 'incidents' will be recorded and dealt with in line with the schools' expectations for behavior.

A connection to the internet can significantly increase the risk that the school network can become affected by a virus or accessed remotely by unauthorized persons. The IT technician is responsible for regularly updating virus protection and will keep up to date with new developments in order to ensure that system security strategies are improved as and when necessary. In common with other media, some material available on the internet is unsuitable for students. The school will take all reasonable precautions to ensure that students may only access appropriate material.

Curriculum

All students in the school will learn about E-safety at their appropriate level of learning and engagement. Staff will adapt the curriculum map to suit individuals and personalise their learning. Staff will select learning materials that are appropriate the age, group, interests and learning style of the students. Elements of the E-safety curriculum can also be found in the Citizenship and PSHE curriculum and KS5 curriculum around personal safety.

Cyberbullying

Cyberbullying is best defined “The use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else”. DCSF 2009

Cyberbullying along with any other forms of bullying by a member of the school community will not be tolerated and will be dealt with in line with the school anti-bullying policy.

Students will learn about cyberbullying as part of the school curriculum. They will consider the impacts and consequences through separate safety lessons.

Personal use of the internet and computers by staff

During the school day staff should not access the internet using school computers or laptops for personal reasons. The IT technician have the right to monitor individual usage and report any concerns to the Headteacher and safeguarding lead. For further information please refer to Staff Acceptable Use Policy and Social Media Guidance.

Any damage to school lCT equipment must be reported to the IT technician immediately by emailing the helpdesk.

All laptops and class iPads must be handed to the IT technician on a termly basis for general maintenance purposes; which could include inspections, tests, replacement of hardware, installation of new software or cabling, as well as for any other reasonable purpose.

School Website and content

The aim of the school website is to promote the school, enhance communication and publish information, and celebrate student’s achievements. The overall editorial responsibility lies with the Headteacher who will ensure that the content is accurate and appropriate.

- Photographs used on the website that include students, will only be published after being carefully selected.
- Permission to use images will be obtained from parents/carers before images are published. This record will be undated annually or on parent carers request.
- Images and supporting text will not allow individuals to be identified
- Student’s names will not be included anywhere on the website

Working with parents

Parents and carers can access this policy via the school website. Printed copies for those without internet access can be requested. Parents have a key role to play in promoting internet safety by adopting control measures at home and reinforcing the messages taught at school. The school will endeavor to promote internet and E-safety, by advising parents whenever possible though the school website, parent/staff conversations and links sent by ‘Class dojo’.

Managing Information Systems

Maintaining Information Systems Security

- The security of the school information systems and users will be reviewed regularly
- Virus protection will be updated regularly
- Portable media may not be used without specific permission alongside an anti-virus/malware scan on a regular basis.
- Unapproved software will not be allowed in work areas or attached to email
- Files held on the school's network will be regularly checked
- The network manager will review system capacity regularly
- Use of user logins and passwords to access the school network will be enforced.

Password Security

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies)
- Access to personal data is securely controlled in line with the school's personal data policy
- Logs are maintained of access by users and of their actions while users of the system

A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems including email.

The management of password security will be the responsibility of the IT Technicians. See the password policy for further detail.

Responsibilities

All staff will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Any changes carried out must be notified to the member of staff responsible for issuing and coordinating password security. Users will change their passwords every 6 months. Staff will also be expected to be up to date with the GDPR recommendations and have read and been briefed on the school policy concerning all aspects of it.

Training/Awareness

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss.

Members of staff will be made aware of the school's password security procedures:

- At induction
- Through the school's E-Safety policy
- Through the Acceptable Use Agreement

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Technician.

Audit/Monitoring/Reporting/Review

The IT Technician will monitor and maintain a log of the use of the internet and other forms of information technologies, any evidence of misuse will be reported to the Headteacher immediately.

The network manager will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner (safe).

Email and Class Dojo

All staff will be given a school email account for the purpose of school business.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

School email accounts should not be used for communication with parents unless approved by a member of the senior leadership team. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

All emails should be written and checked carefully before sending, in the same way as a letter sent on school headed paper.

When sending emails to external organisations staff are advised to CC. their line manager or the Headteacher.

Confidential information should never be sent. Where information needs to be sent via email staff must:

- depersonalise the communication

- encrypted storage devices must be used for transporting confidential information.
- encrypt any documentation using an appropriate AES encryption process.
- verify the details, including accurate e-mail address, of any intended recipient of the information
- verify (by phoning) the details of a requestor before responding to e-mail requests for information
- not copy or forward the e-mail to any more recipients than is absolutely necessary
- not send information to any body/person whose details have not been separately verified (usually by phone)

Class staff will have access to Class Dojo for their teaching group. It is an interactive form of instant communication between staff and parents to share learning information. Staff will only share learning and information directly with the student's parents. **(Class Dojo Guidance for parents 2021)**

Personal Information

> 'Personally identifiable **information** (PII), or sensitive **personal information** (SPI), as used in **information** security and privacy laws, is **information** that can be used on its own or with other **information** to identify, contact, or locate a single person, or to identify an individual in context.'

It is the responsibility of all staff using such information, to ensure that it is password protected and, in some cases, encrypted on school devices. Should it need to be 'transported' then school encrypted memory devices must be used. Once this information has been used it will be removed from such devices.

Use of video and digital images

As a school we recognise the educational benefits that the development of video digital imaging technologies has on learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. Therefore, with the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

It is the responsibility of school staff to ensure that video/digital images are taken only to promote educational purposes or to record and celebrate student achievement.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. Only school devices can be used.

At certain times teachers will find it necessary to store photographs on pen drives and laptops to enable them to fulfill their duties, such activities may include writing school reports, collating records of achievement or preparing work samples for moderation. However, once the work has been completed all images must be deleted immediately. All photograph must be stored on password protected or encrypted devices.

Images may be stored on the school network for educational purposes only and will be reviewed regularly by the IT technicians.

Responding to incidents of concern

All staff must report to the Headteacher immediately should they have any concerns regarding inappropriate use of the internet or any other form of information technology. The Headteacher will undertake the appropriate investigation as soon as possible.

The Designated Person for Child Protection will be informed of any E-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

The school will inform parents/carers of any incidents of concerns as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

Where there is cause for concern that illegal activity has taken place or is taking place then the school will contact Children's Services and escalate the concern to the Police.

A log will be maintained of all incidents and reviewed regularly by SLT and governors.

Related policies

GDPR Policy
Password Policy
Child protection
Data security
Anti-bullying
Social Media Guidance
Acceptable User Policy
Class Dojo Guidance for parents