Benfield School
E-SAFETY POLICY

Contents

1. What is E-Safety?

Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young students. Some examples of this are:

• Bullying or harassment via chat or email

• Obsessive internet use
• Exposure to inappropriate materials
• Inappropriate or illegal behaviour
• Physical danger of sexual abuse

As a school, it is our duty of care alongside that of parents and other members of the community to protect our children from these dangers and this can be achieved by many different mechanisms working together.

The purpose of this e-safety policy is to outline what measures we take to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion. This policy guidance aims to help everyone at Benfield School understand their roles and responsibilities in ensuring the safe and acceptable handling/use of information technologies.

2. General policy statement

The school will endeavour to ensure the e-safety of all school members. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

3. Roles and Responsibilities

Within school all members of staff and students are responsible for e-safety, responsibilities for each group include:

Students

• Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety training sessions.

• Compliance with a highly visible student's Acceptable Use Policy (AUP) which students must agree to each time they use academy ICT equipment either in the academy or remotely which connects to the internet.

• Reporting any e-safety issue to the teacher, welfare staff or parent.

• Take responsibility for their own actions using the internet and communications technologies.

All Staff

• Have a clear understanding of e-safety issues and the required actions from e-safety training sessions.

• Reporting any e-safety issues to the E-Safety (safeguarding) manager as soon as the issue is detected.

• Compliance with a highly visible staff Acceptable Use Policy (AUP) which staff must agree to each time they use school ICT equipment either in the school or remotely which connects to the internet.

Care must be taken whenever staff choose to use their own personal technologies in school and they must ensure that other people, including children, are not able to see personal content which would be deemed private or sensitive (keeping professional and private lives separate).

Deliberate unlawful, inappropriate material must not be viewed, stored or distributed on the school system.

Teaching Staff

• Educating students on e-safety through specific e-safety training sessions and reinforcing this training in the day to day use of ICT in the classroom.

Network Manager (Alan Vowles)

• Ensure that the best technological solutions are in place to ensure e-safety as well as possible whilst still enabling students to use the internet effectively in their learning.

• Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition, securing and preserving evidence of any e-safety breach.

• Checks and audits all systems to ensure that no inappropriate data is stored or is accessible.

• Works with the ICT Director to create, review and advise on e-safety and acceptable use policies.

ICT Director (Karena James)

• Leads the development of the e-safety education programme for students and staff.

• Manages parental awareness for e-safety.

E-Safety (Safeguarding) Manager (Maria Irving)

• Deals with e-safety breaches from reporting through to resolution in conjunction with the ICT support team.

• Works with the ICT Manager and ICT Director to create, review and advise on e-safety and acceptable use policies.

• Works with outside agencies including the police where appropriate.

• Maintains a log of all e-safety issues.

ICT Support Team

• Monitors the technology systems which track student internet use to detect e-safety breaches.

• Assists in the resolution of e-safety issues with the E-Safety Manager and other members of staff.

The Headteacher is ultimately responsible for network activity and e-safety in the school.

5. How we ensure e-safety in the classroom

Educating students in e-safety

A clear objective of the school is to educate students in safe use of ICT and the internet. We feel this is one of the best ways to minimise the potential for any e-safety issues to occur.

Students will receive specific e-safety lessons aimed at ensuring that:

• Students know the e-safety risks that exists and how to identify when they are at risk.

• Students know how to mitigate against e-safety risks by using e-safe practices whilst online.

• Students know when, how and to whom to report instances when their e-safety may have been compromised.

• Students know that they are in an environment that encourages them to report e-safety issues without risk of reprimand, humiliation or embarrassment.

All members of staff have a duty to reinforce e-safety practices wherever possible and will offer students advice and support in the classroom where minor e-safety incidents have occurred.

Acceptable Use Policies

All school members both students, staff and parents must follow an Acceptable Use Policy (AUP) to use school ICT systems. With respect to e-safety the AUP details:

• The user's responsibilities

• Activities which are appropriate and inappropriate

• Best practice guidelines

• How the school will monitor e-safety

• What information is collected

How e-safety is monitored

• The ICT support team will actively monitor student ICT activity using a monitoring system which can flag potential e-safety issues.

• The ICT team will periodically review internet access logs to track any websites which could potentially present an e-safety issue.

• The E-Safety manager will periodically review the E-Safety log to track and trends and use the information to look at ways of improving the student's e-safety.

• Teaching staff will directly monitor student ICT and internet use in the classroom.

How technology is used

School employ many different technologies to help to ensure e-safety for all the academy members:

• School will use internet filtering to block inappropriate content as designated by the DFE and Becta and in addition block websites which are irrelevant to the student's programme of study and are considered time wasting.

• School will use a system which tracks all student activity on the academy's computers. This system will automatically flag potential e-safety issues which will be monitored and then can be investigated by the support for learning team.

• School will restrict which activities the students can perform using ICT and the internet through systems security policy and access control.

• Teaching staff will use control mechanisms to attempt to limit the applications and web sites which the students can visit whilst using ICT within a lesson.

6. How we will respond to issues of misuse

The following are provided for the purpose of example only. Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Headteacher.

Students:

Level 1 infringements

• Use of non-educational sites during lessons • Unauthorised use of email • Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: IRIS /removal of phone until end of day / contact with parent/ removal of Internet access rights for a period]

Level 2 infringements

• Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email after being warned • Continued unauthorised use of mobile phone (or other new technologies) after being warned • Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: IRIS / referred to Year Leader or SLT / e-safety Manager / removal of phone to be collected by parent / contact with parent / removal of Internet access rights for an extended period / internal exclusion]

Level 3 infringements

• Deliberately corrupting or destroying someone's data, violating privacy of others • Sending an email that is regarded as harassment or of a bullying nature (one-off) • Deliberately trying to access

offensive or pornographic material • Any purchasing or ordering of items over the Internet
• Transmission of commercial or advertising material

[Possible Sanctions: IRIS / referred to SLT and Headteacher informed / e-safety Manager / contact with parents / removal of equipment/ removal of Internet for an extended period/ exclusion/ referral to police]

Level 4 infringements

• Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned • Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 • Bringing the school name into disrepute

[Possible Sanctions – IRIS / Referred to e-safety Manager/ Headteacher /exclusion / removal of equipment / referral to police / LA safeguarding officer.

Staff:

Level 1 infringements (Misconduct)

• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. • Misuse of first level data security, e.g. wrongful use of passwords • Breaching copyright or license e.g. installing unlicensed software on network

[Sanction - referred to line manager / Headteacher / Warning given.]

Level 2 infringements (Gross Misconduct)

• Serious misuse of, or deliberate damage to, any school computer hardware or software; • Any deliberate attempt to breach data protection or computer security rules; • Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; • Bringing the school into disrepute.

[Sanction – referred to Headteacher who will follow school disciplinary procedures / Police / Governors]

Child Pornography:

In the case of child pornography being found, the member of staff will be immediately suspended and the school disciplinary procedures implemented.

Other safeguarding actions:

• Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
• Instigate an audit of all ICT equipment to ensure there is no risk of pupils accessing inappropriate materials in the school. • Identify the precise details of the material. • Where appropriate, involve external agencies as part of these investigations.

How will staff and students be informed of these procedures?

• Procedures are included within the school's e-safety / Acceptable Use Policy. All staff are required to sign the school's e-safety Policy acceptance form; • Pupils will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviours'. Pupils are required to sign an

age appropriate e-safety / acceptable use form; • The school's e-safety policy will be made available to parents who are required to sign an acceptance form when their child starts at the school. • Staff are issued with the 'What to do if?' guide on e-safety issues.

6. Working with parents and the community

Clearly many academy students will also have access to ICT and the internet at home, often without some of the safeguards that are presents within the academy environment. Therefore, parents must often be extra vigilant about their child's e-safety at home.

One of our goals is to support parents to provide an e-safe environment for their children to work in outside of school.

We will do this in several ways;

• Run training sessions and workshops on e-safety

• Publish e-safety information and direct parents to external e-safety advisories via the school website.

Data Protection

We record data and information about pupils, staff and other resources. This makes us a 'data controller' and means we must adhere to a set of key principles when using data and information.

Data Protection Act 1998 (DPA)

The DPA is a legal framework for collecting, storing and processing personal data. It is underpinned by eight data protection principles which we as a data controller must comply with.

Personal data must be:

- processed fairly and lawfully;
- processed for specified purposes;
- adequate, relevant and not excessive;
- accurate and kept up to date;
- disposed of securely when no longer needed;
- processed in line with the rights of the individual (right of access, right to have inaccurate information corrected, right to prevent processing likely to cause damage and/or distress);
- kept secure;
- not transferred outside the European Economic Area unless adequately protected.

Further information on the Data Protection Act be found at: www.ico.gov.uk

Photographing Children

The definition of personal data extends to photographs of children taken by school staff or others on their behalf (e.g. professional photographers). We seek informed consent from parents in relation to the taking and using of such photographs. We do this is at the beginning of a new school year or on enrolment. Photographs are stored on secure drives and not left on devices.

Recommended Good Practice

The Data Protection Act is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure.

Where the Act does apply, a common-sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

Photos taken for official school use may be covered by the Act and pupils and students should be advised why they are being taken.

Photos taken purely for personal use are exempt from the Act.

Examples:

Personal use:

- A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.
- Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.

Official school use:

- Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.
- A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used.

Media use:

A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act.

Subject Access Requests

Data subjects (including pupils and parents) have a right of access to information held about them. In such cases, they should submit a written request to the school stating clearly what they wish to access. In most cases copies of educational records must be provided with 15 working days and any other personal data within 40 working days. A child's information must only be released to a parent/guardian where such a disclosure is in the best interest of the child.

Usually, data should only be released to the person it relates to. In the case of young children, data can be released to parents without the child's permission. The DPA doesn't define the age at which a child is deemed to be able to take over responsibility for their own data from their parents, but the guidance suggests age 12 is usually a reasonable point. However, this may differ and cases should be considered carefully and individually.

Under the Act, a pupil, or someone acting on their behalf, has the right to access their personal information held by the school. This includes:

- information held on computer (or other automated means);
- information held in structured files;
- information in their educational record; and
- unstructured information, for example, held in loose correspondence

Freedom of Information Act 2000 (FOIA)

The FOIA provides the public with a right of access to official information. People are often unsure about the difference between FOIA and DPA. Broadly speaking, the FOI covers information on resources, aggregated information about individuals and performance information and the DPA applies to data about individuals. For example, an FOIA request might include the number of staff employed, the percentage of days lost through sickness or attainment data. When considering an FOIA request for information, the DPA takes precedence. Therefore, if information requested under the FOIA could be used to derive information about specific individuals (and therefore is covered by the DPA), then the FOIA request can be refused. If in any doubt, seek advice.

Dealing with FOI requests

We are under a duty to provide advice and assistance to anyone requesting information. The enquirer is entitled to be told whether the school holds the information, except where certain exemptions apply. Requests should be dealt with within 20 working days excluding school holidays.

A valid FOI request should be in writing (and can include one made via an email), state the enquirer's name and correspondence address and describe the information requested. Expressions of dissatisfaction should be handled through the school's existing complaints procedure.

Policy updated: September 2016