Internet Safety Policy

Version 1.0

Important: This document can only be considered valid when viewed on the Trust's website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.	
Name of Author	Trust ICT Development Manager
Name of Responsible Committee/Individual	Trust Board
Implementation Date	July 2021
Review Date	September 2022
Target Audience	All Stakeholders
Related Documents	Acceptable Use Agreement - Staff Acceptable Use Agreement – Parent/Student Code of Conduct Social Media Policy Data Protection Policy

CONTENTS

1. RATIONALE

Digital technologies have become integral to the lives of children and young people, both within and out of school. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and provide a context for effective learning. Young people should have an entitlement to safe internet access at all times. It is therefore essential that, with the use of these new technologies, staff, students/pupils and parents for schools/college in the Brighter Futures Learning Academy Trust are aware of the relative dangers and some of the legal implications of misuse.

2. PURPOSE AND SCOPE

The internet safety policy aims to create an environment where all stakeholders including the wider community work together to inform each other of ways to use the internet responsibly, safely and positively.

Students/pupils, staff and all other users of trust and school related technologies should work together to agree a set of standards and expectations relating to appropriate usage by promoting safe and responsible access.

The policy is not designed to be a blacklist of prohibited activities, but instead a guide to appropriate use, leading to safer internet usage. It is intended that the positive effects of the policy will be seen on and offline; in school and at home; and ultimately beyond school and into the workplace.

This policy applies to all schools/college in the Trust.

3. ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for all stakeholders.

CEO and Trustees

Will be responsible for approving this policy and ensuring it is reviewed each year. It will also monitor and evaluate the effectiveness of its implementation.

School Governors, the Headteacher/Principal and the School's/College's Strategic Leads for ICT

Will be responsible for the implementation of the Internet Safety Policy and for monitoring the effectiveness of the policy.

School Senior Leaders

The School's/UTC's senior leaders will:

- Be responsible for ensuring internet safety of members of the school/college.
- Be responsible for ensuring that relevant staff receive suitable training and development to enable them to carry out their internet safety roles and to train other colleagues, as relevant.
- Ensure that there is a system in place to allow for the monitoring and support of those in the school who carry out the internal internet safety monitoring role. This is to provide a safety net and to support key personnel who take on important monitoring roles.
- Receive information regarding any internet safety incidents which will be logged by the central IT Team or Senior Leader responsible for IT and be reviewed during SLT meetings.

- Be aware of the procedures to be followed in the event of a serious internet safety allegation being made against a member of staff ensuing all breaches are reported to the Headteacher and where appropriate, the Central Trust.

Members of School's/College's Senior Leadership Teams with responsibility for internet safety

They will:

- Take day to day responsibility for internet safety issues and oversee the sanctions for breaches of rules relating to internet safety.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an internet safety incident taking place.
- Provide training and advice to staff.
- Liaise with the Local Authority Designated Officer (LADO) or Police as appropriate.
- Liaise with and support the Trust's ICT technical staff.
- Ensure regular reporting of internet safety incidents to School SLT as part of behaviour monitoring.
- Provide information to the Headteacher/Principal and Governors as appropriate.
- **Ensure all serious breaches are reported into the Trust immediately**

Trust ICT Department

The Trust ICT Manager, ICT Development Manager and ICT Technicians will, except where schools currently purchase a 'bought-in' service' which addresses all areas of ICT security:

- Ensure that the Trust and School/UTC ICT infrastructure is secure and is not open to misuse or malicious attack and that all aspects of the Trust and School's /UTC's ICT systems are secure, in line with the Trust's guidance and policies.
- Put in place appropriate filtering and monitoring systems (including any 'Bring your own device, or BYOD access system'), which are updated on a regular basis and keep students/pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material in-line with the PREVENT agenda.
- Ensure that the Trust and School/UTC ICT systems (including those that are cloud based) are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conduct a full security check and monitor the Trust's and School's/College's ICT systems on a weekly basis.
- Take appropriate measures to block access to potentially dangerous content and, where possible, prevent the downloading of potentially dangerous files.
- Ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensure that any incidents of cyber-bullying are dealt with appropriately and in line with the school behaviour policy.

If schools or the college purchase the services of external providers then Headteachers/Principals and the Local Governing Board must ensure appropriate security and ensure that their systems are secure and protected against viruses and malware.

Staff

Staff will:

- Have an up-to-date awareness of e-safety matters and of the Trust's current Internet Safety Policy and practices.
- Have read and understood the Social Media Policy and signed the ICT Acceptable Use Agreement.
- Ensure internet safety issues are embedded in all aspects of the curriculum and other school activities.
- Ensure students/pupils understand and follow the Trust's internet safety policy and ICT Acceptable Use Agreement.
- Ensure students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Ensure they monitor ICT activity in lessons, extra-curricular and extended school activities.
- Ensure they are aware of internet safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current best practice regarding these devices.
- Ensure that in lessons where internet use is pre-planned, students/pupils should be guided to sites that are checked as suitable for their use and that processes are in place to deal with any unsuitable material that is found in internet searches.
- Report any suspected misuse or problem to a member of SLT and Trust ICT Support.
- Ensure that digital communications with students are only on a professional level and carried out using official school systems.
- Maintain a formal and courteous and professional tone in communicating with students/pupils and ensure that professional boundaries are always maintained.
- Only use official channels of communication e.g., Office 365, Microsoft Teams and work e-mail addresses and be aware of and comply with the Trust's policies and guidance.
- Staff will not use their personal mobile phone on site without the express permission of the Headteacher/Principal.

The Trust uses filtered services and will endeavour to ensure that inappropriate material is not accessible by students/pupils. However, any staff with knowledge of inappropriate sites available through the filtered access should inform the ICT Support Manager or Senior Leader as a matter of urgency. **The Trust nor School/College cannot accept any liability for accessing inappropriate content.**

Designated Safeguarding Leads

Should be trained in internet safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.
- PREVENT

Students/Pupils

Pupils/Students will ensure that:

- They are responsible for using the ICT systems in accordance with the Trust policies, which they will be expected to sign an Acceptable Use Agreement before being given access to the ICT systems.
- They have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They should understand the importance of adopting good internet safety practice when using digital technologies out of school and realise that the Trust's internet safety policy covers their actions out of school, if related to their membership of the school.
- In Secondary schools/UTCs the Trust's schools, students/pupils are responsible for ensuring digital devices, including mobile phones, are not used during the timetabled day. Mobile phones should be switched off and kept in bags/lockers throughout the school day including before school, break, lunchtimes, and movement times. They should not be used until leaving the site at the end of the school day. Further consequences for this action can be found in the school/UTC's behaviour policy.
- **In the Trust's Primary/Infant Schools, pupils are not permitted mobile phones at any time.** If a pupil is required to have a mobile phone to facilitate travel, the phone should be handed into the school office where it will be kept until the end of the school day. The Trust/School accept no liability for personal mobile phones that are brought onto the premises.

Students/pupils must ensure that files stored on their digital devices/phones do not contain inappropriate images e.g., violent, degrading, or offensive. The transmission of some images/information can be a criminal offence and will be dealt with as such by the school.

Responsibility for the digital device/phone rests solely with the student/pupil ; the School/UTC accepts no financial responsibility for damage, loss, theft, or costs incurred when using the phone for any purpose.

Users of Computer Equipment (Both Staff and Students)

Individual users of the Internet are responsible for their behaviour and communications over the network. Users will comply with school/UTC standards and will honour the agreements they have signed.

Users should expect that electronic communications, files stored on servers or other storage media will be open to inspection.

During the school/UTC day, teachers will guide students/pupils toward appropriate materials. Outside of the school/UTC day, families bear responsibility for such guidance and they must also exercise with care, information sources such as television, telephones, movies, radio and other potentially offensive media.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

Parents and carers will be responsible for:

- Endorsing the Trust's Internet Safety and Social Media Policy.
- Accessing the Trust and school websites in accordance with the relevant Acceptable Use Agreement.

- Informing the school/UTC of any concerns arising from the inappropriate use of digital media and the internet.

4. EDUCATION AND TRAINING

Students/Pupils

Internet Safety education will be provided in the following ways:

- A planned internet safety programme will be provided as part of the curriculum.
- Key internet safety messages will be reinforced as part of a planned programme of assemblies and within the curriculum.
- Students/pupils will be taught, whenever an opportunity occurs, to be critically aware of the material/content they access on-line and be guided to validate the accuracy of information.
- Students/pupils will be encouraged to adopt safe and responsible use of ICT, the internet, and mobile devices both within and outside the school.
- Students/pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Internet safety training for all staff is included as part of Level 1 child safeguarding training.
- All new staff will receive internet safety training as part of their induction programme, ensuring they understand the internet safety policy, social media policy and Acceptable Use Agreement – this training is a requirement for all new staff.

Trustees and Governors

Trustees and Governors are required to undertake internet safety training as part of regular, scheduled, safeguarding training.

5. INFRASTRUCTURE, EQUIPMENT, FILTERING AND MONITORING

The Trust's ICT Managers will be responsible for ensuring that the Trust and School's/UTC's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. They will work with Headteachers/Principals and Senior Leaders to ensure that any out-sourced provision is 'fit for purpose:

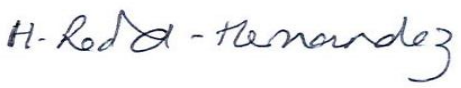
- All users will have clearly defined access rights to ICT systems.
- All users will be provided with a username and password by ICT support who will keep an up-to-date record of users and their usernames. Users will not be required to regularly change their password (in line with guidance on From the National Cyber Security Centre (NCSC) and the Cyber Essentials program) but will be expected to have a complex password.
- Where younger users are not able to have a complex password, their account will be very limited in their access privileges so ensure privacy and compliance with the Data Protection Policy.
- Users will be made responsible 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.

- In the event of the ICT Manager (or other member of the IT Support Team) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher/Principal in all occasions incidents must be logged and reported to the CEO.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Manager, and where a third party provider is used for internet filtering, the Trust ICT Manager must be informed of any changes.
- ICT technical staff regularly monitor and record the activity of users on the ICT systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users' activity.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc from accidental or malicious attempts which might threaten the security of the systems and data.
- Guest users may be granted a temporary log in or guest account if agreed by the Headteacher/Principal and ICT Manager.
- Personal use of the ICT systems should be limited to what may be deemed reasonable. The services are provided predominantly for education purposes. Any costs associated with printing will be charged to the individual member of staff.
- Neither staff nor students/pupils should install programmes, run scripts or other software on workstations, portable devices, or servers, without the prior express permission of the ICT Manager.
- The ICT infrastructure and individual workstations are protected by up-to-date anti-virus software.
- Personal data (as defined by the Data Protection Act 2018) must not be sent over the internet or taken off school premises or from school systems. Where there is an educational reason to pass personal details to a third party this will be logged and approved by the Data Protection Officer (DPO) and Trust IT Manager only.
- ICT will maintain an email security system that reduces the amount of fake and phishing emails. Staff will however need to be vigilant and report any suspected emails. Appropriate training will also be provided to all staff on identifying and dealing with fake and phishing emails.

Information will be reviewed and updated on an annual basis to ensure that the information remains current.

Internet Safety Policy Agreed: July 2021 (Version 1)

Signed CEO of BFLPT – Helen-Redford-Hernandez:



Date: July 2021

Signed – Chair of BFLPT – Marcus Isman-Egal:

Date: July 2021

Internet Safety Policy to be reviewed : September 2022

Created: July 2021 (Version 1)

Revised: