Digital Safety Policy

Version 9.0

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 Manager
Name of Responsible Committee/Individual	Trust Board
Date Policy Agreed	April 2021 (Version 1) (formally Internet Safety) May 2022 (Version 2) (formally Internet Safety) July 2022 (Version 3) (formally Internet Safety) December 2022 (Version 4) (formally Internet Safety) March 2023 (Version 5) (new name Digital Safety) July 2023 (Version 6) July 2024 (Version 7) July 2025 (Version 8) March 2026 (Version 9)
Review Date	July 2026
Target Audience	All Stakeholders
Related Documents	Acceptable Use Agreement - Staff Acceptable Use Agreement – Parent/Student AI Policy 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 always have an entitlement to safe internet access. It is therefore essential that, with the use of these new technologies, staff, students, and parents for schools in the Brighter Futures Learning Academy Trust are aware of the relative dangers and some of the legal implications of misuse.

The Trust recognises the increasing use of Artificial Intelligence (AI), including generative AI tools, in education and wider society. While AI presents opportunities to enhance learning and productivity, it also introduces safeguarding, data protection, misinformation and assessment integrity risks. The Trust's approach to AI is governed by its separate Artificial Intelligence (AI) Policy, which must be read alongside this Digital Safety Policy.

2. PURPOSE

The Digital 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 IT and digital facilities responsibly, safely, and positively.

Students, 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 usage of IT and digital facilities. 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.

3. ROLES AND RESPONSIBILITIES

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

Trust CEO, Trust Board and Trustees

Responsible for ensuring policies are maintained and checked each year and each school is implementing the policies. Also responsible for regularly reviewing the effectiveness of web filtering and ICT monitoring systems across the Trust.

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

Be responsible for the implementation of the Digital Safety Policy and for monitoring the effectiveness of the policy. Also responsible for regularly reviewing the effectiveness of web filtering and ICT monitoring systems within their schools and ensuring that the leadership team and relevant staff have an awareness and understanding of the provisions in place. Also responsible for ensuring that all staff undergo safeguarding and child protection training (including online safety).

School Senior Leaders

The school's senior leaders will:

- Be responsible for ensuring the digital safety of members of their school.
- Be responsible for ensuring that relevant staff receive suitable training and development to enable them to carry out their digital safety roles and to train other colleagues, as relevant.
- Be aware of and understand the ICT filtering and monitoring systems in place.
- 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 digital 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 digital safety incidents which will be logged and reviewed during SLT meetings.
- Be aware of the procedures to be followed in the event of a digital/e-safety safety concern.

Members of School's Senior Leadership Teams with responsibility for digital safety

They will:

- Take day to day responsibility for digital safety issues and oversee the sanctions for breaches of rules relating to digital safety.
- Ensure that all staff are aware of the procedures that need to be followed in the event of a digital safety incident taking place.
- Ensure staff receive appropriate safeguarding and child protection training (including online safety) Additionally, all staff should receive safeguarding and child protection updated at least annually.
- 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 digital safety incidents to School SLT as part of behaviour monitoring.
- Provide information to the Headteacher/Principal and Governors as appropriate.

Trust ICT Department

The Trust ICT Manager, Assistant ICT Manager, and ICT Technicians will:

- Ensure that the Trust and School ICT infrastructure is secure and is not open to misuse or malicious attack and that all aspects of the Trust and School's ICT systems are secure, in line with the Trust's guidance and policies.
- Ensure that multi-factor authentication is implemented and enforced where appropriate across Trust systems and services.
- 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 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 ICT filtering and monitoring systems are being managed effectively.
- Ensure that the Trust and School 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 and School'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 digital 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.

Staff

Staff will:

- Have an up-to-date awareness of e-safety matters and of the trust's current Digital Safety Policy and practices.
- Have read and understood the Social Media Policy and signed the ICT Acceptable Use Agreement.
- Ensure digital safety issues are embedded in all aspects of the curriculum and other school activities.
- Ensure students understand and follow the Trust's digital safety policy and ICT Acceptable Use Agreement.
- Ensure students 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 digital 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 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 team.
- 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 and ensure that professional boundaries are always maintained.
- Only use official channels of communication e.g., Office 365, home learning platforms, and work e-mail addresses and be aware of and comply with the Trust's policies and guidance.
- Comply with the Trust's multi-factor authentication requirements and take reasonable steps to secure any personal device used for authentication.
- Ensure that any use of Artificial Intelligence tools is in line with the Trust's Artificial Intelligence (AI) Policy.
- Not input personal, safeguarding or confidential data into AI platforms unless authorised and risk assessed.
- Maintain professional responsibility and oversight for any AI-generated content used in teaching, assessment, decision-making or communication.

All schools use a filtered service and will endeavour to ensure that inappropriate material is not accessible by students. However, any staff with knowledge of inappropriate sites available through the filtered access should inform the Trust ICT Manager as a matter of urgency. The Trust nor School can accept any liability for accessing inappropriate content.

Designated Safeguarding Leads

Should be trained in digital safety/e-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
- The misuse of Artificial Intelligence tools, including the creation of deepfakes, manipulated images, or AI-generated harmful content.

Designated Safeguarding Leads will:

- Take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems in place).

Students

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 for 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 digital safety practice when using digital technologies out of school and realise that the Trust's digital safety policy covers their actions out of school, if related to their membership of the school.
- They are responsible for ensuring digital devices, including but not limited to, mobile phones, tablets, smart watches, are only used with the permission of the teacher. Mobile phones should be switched off and kept in bags 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.
- Use Artificial Intelligence (AI) tools only in accordance with the ICT Acceptable Use Agreement and Artificial Intelligence Policy and guidance provided by staff.
- Not use AI tools to complete assessed work unless explicitly permitted.
- Understand the risks of misinformation, bias, and inaccuracy in AI-generated content.

Students 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, the Trust and School accepts no financial responsibility for damage, loss, theft, or costs incurred when using the digital devices/phones for any purpose.

Users of Computer Equipment (Both Staff and Students)

Individual users of the IT and digital facilities are responsible for their behaviour and communications over the network. Users will comply with school 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 school, teachers will guide students toward appropriate materials. Outside of school, 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 school's Digital Safety and Social Media Policy.
- Accessing the Trust and school websites in accordance with the relevant Acceptable Use Agreement.
- Informing the school of any concerns arising from the inappropriate use of digital media and the internet.

4. EDUCATION AND TRAINING

Students

Digital Safety education will be provided in the following ways:

- A planned digital safety/e-safety programme will be provided as part of the curriculum.
- Key digital safety messages will be reinforced as part of a planned programme of assemblies and within the curriculum.
- Students 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 will be encouraged to adopt safe and responsible use of IT, the internet, and mobile devices both within and outside the school.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students will be educated on the safe, ethical and responsible use of Artificial Intelligence tools, including understanding bias, misinformation, data privacy and academic integrity.

Staff

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

- Digital safety training for all staff is included as part of Level 1 child safeguarding training.
- All new staff will receive digital safety training as part of their induction programme, ensuring they understand the Digital Safety Policy, Social Media Policy, Artificial Intelligence Policy and Acceptable Use Agreement.
- Staff will receive guidance on the appropriate use of Artificial Intelligence in line with the Trust AI Policy.

Governors

Governors are required to undertake digital safety training as part of regular, scheduled, safeguarding training.

5. INFRASTRUCTURE, EQUIPMENT, FILTERING AND MONITORING

The Trust ICT department will be responsible for ensuring that the Trust and School's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- All users will have clearly defined access rights to ICT systems.
- All users will be provided with a username and password by the Trust ICT team 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 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 to 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.
- Where available, access to Trust and School systems will be protected using multi-factor authentication (MFA) in addition to a username and password. MFA provides an additional layer of security by requiring users to verify their identity using a second factor, such as an authenticator application or approved verification method.
- MFA will be enforced for access to cloud-based services, remote access systems, and any other systems deemed to present an increased security risk.
- Users are aware that all ICT services are monitored and filtered and logs will be made available to Trust Leaders or School Senior Leaders in the event of misconduct or policy breaches.
- Users are aware that school devices are actively monitored for safeguarding purposes. Safeguarding concerns will be made available to the Designated Safeguarding Leads.
- Where appropriate, AI tools and platforms will be risk assessed and subject to filtering and monitoring controls in line with safeguarding requirements.
- In the event of the Trust 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/Trust CEO.
- Requests from staff for sites to be removed from the filtered list will be considered by the Trust ICT Manager.
- 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 Trust 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.
- Neither staff nor students should install programmes, run scripts or other software on workstations, portable devices, or servers, without the prior express permission of the Trust ICT Manager.
- The ICT infrastructure and individual workstations are protected by up-to-date anti-virus software.
- The Trust ICT team ensures that all critical systems and data are regularly backed up, and that backups are encrypted, tested periodically, and stored in a separate physical or cloud environment to prevent unauthorised access.
- 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 ICT Manager only.

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

6. CYBER SECURITY

Cyber Security is of the utmost importance to the Trust and all users must follow the guidance to the procedures and practices listed below.

Emails

Emails are the most common form of cyber-attacks via phishing scams, ransomware attacks, malicious software attachments. Users must ensure to:

- Avoid opening attachments or links from suspicious emails
- Seek clarification from the Trust ICT team if the user receives an email with an attachment or link that they are not expecting or if the sender is not legitimate.
- Any suspicious emails or attachments are forwarded to the Trust ICT team immediately.
- Where users have email accounts and other Trust/School data on a personal device, they must ensure that the device is locked with a password.
- The user must inform the Trust ICT team immediately if they believe they have been victim to a cyber-attack.

Passwords

Any password leak or weak password could compromise an ICT infrastructure. Users must ensure to:

- Use strong passwords in accordance with the National Cyber Security Centre (NCSC) password policy guidance.
- Avoid using information in their passwords that can be easily guessed (birthdays, family names, pet names, etc).
- Avoid writing passwords down.
- Avoid changing their password regularly. The guidance from the National Cyber Security Centre (NCSC) now advises users to only change their password if they suspect that they may have been compromised.

Multi-Factor Authentication (MFA)

The Trust requires the use of multi-factor authentication (MFA) to protect systems and data from unauthorised access, account compromise, and cyber-attacks such as phishing.

Where required, staff may need to use an authenticator application on a personal device to verify sign-in attempts. This application is used solely to confirm identity and does not provide the Trust with access to personal data stored on the device.

Staff must ensure that any personal device used for authentication is protected with a password, PIN, biometric lock, or equivalent security measure. Any device used for authentication that is lost, stolen, or believed to be compromised must be reported immediately to the Trust ICT team so that access can be secured.

Data Storage/Transfer

The storage and transferring of data can pose a security risk. Users must ensure to:

- Avoid storage sensitive data (data that contains personal records and information) on personal devices.
- Avoid using USB Storage devices. Where USB Storage Devices are used, these must be encrypted.
- Use School/Trust provided platforms (Microsoft 365) to store data.
- Avoid transferring sensitive data where possible. When transferring of sensitive data is necessary, users must use School/Trust provided platforms (Microsoft 365) and seek the support of the Trust ICT team.
- Report any suspicious activity, data breaches, cyber attacking attempts to the Trust ICT team immediately.
- Users must not input personal data, safeguarding information or confidential Trust information into publicly available Artificial Intelligence systems unless explicitly authorised and risk assessed.

Additional Guidance

To further protect our infrastructures, services, and data, we ask our users to:

- Lock their device when not in use.
- Lock their offices/classrooms when not in use, if possible.
- Ensure passwords are not written down and visible to other users.
- Report any suspicious activity or potential cyber-attack to the Trust ICT team immediately.
- Report any potential security weakness in the ICT infrastructure immediately.
- Refrain from trying to install software on Trust devices or attempting to bypass ICT systems in any way.
- Report stolen equipment as soon as possible to the Trust ICT team.
- Ensure all passwords are changed in the event of equipment loss or any suspected cyber attack where the password may be compromised.

IT Infrastructure Measures

The Trust ICT team will ensure that:

- Ensure that firewalls, filtering, antivirus software are running on all IT infrastructure systems/services.
- Inform staff of any new trending phishing/malicious threats and scams.

- Ensure Multi-Factor Authentication is being used for all staff where possible.
- Ensure cyber security training is given as part of induction for new staff.
- Ensure cyber security training is renewed annually in line with the 'National Cyber Security Centre – Cyber Security Training for School Staff' material.
- Ensure that all disposed IT equipment is recycled through a registered recycling company and data destruction certificates are provided.
- Ensure regular vulnerability assessments are carried out on core systems, and any critical findings are actioned within appropriate timeframes based on risk.
- The Trust will carry out regular simulated phishing campaigns and/or cybersecurity quizzes as well as termly Cyber Security Awareness emails to test and reinforce staff awareness of cyber risks.

Digital Safety Policy Version 9 agreed by Trust Board 25 March 2026