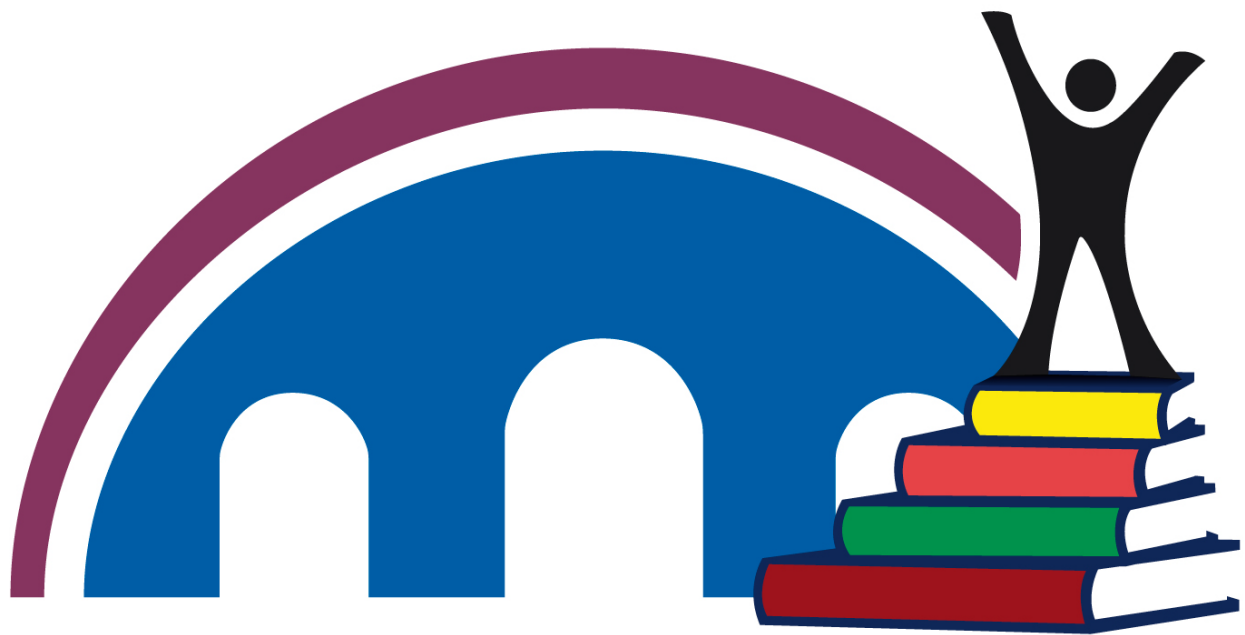




Bridge Academy Trust

IT POLICY STAFF AND STUDENTS

September 2026

Summary of Changes

Section Number	Current wording	Proposed Amendment
1. Introduction		Remove 1.3 to new section scope
2. Scope		New section
3. Roles and Responsibilities		New section
4. Equality Impact Assessment		New Section
Section 10		Removed sentence and added the wording "Refer to the AI Policy".

Date of Draft Policy: (this is the month/year the policy was drafted)	March 2026	
Last approved version Frequency of review	17 th June 2025 Annually	
Consultation with Staff Required	Yes ☐	No ☒
Period of Consultation (if required)	From N/A	To N/A
Trustees Committee Reviewing Document	Trustee Policy Review Committee	
Date of Board of Trustees Meeting at which Policy Approved	16 th June 2026	
Date of Adoption of Policy	1 st September 2026	
Date Policy available on Central Area/www (If appropriate)	1 st September 2026	
Reviewer	Data Protection Officer	
Advice From	The Key	

CONTENTS

INTRODUCTION	1
SCOPE	1
ROLES AND RESPONSIBILITIES	1
BOARD OF TRUSTEES	1
BRIDGE EXECUTIVE BOARD (BEB)	1
CHIEF FINANCE & OPERATIONS OFFICER (CFOO)	1
DIRECTOR OF IT	2
DATA PROTECTION OFFICER (DPO).....	2
HEADTEACHERS / HEADS OF SCHOOL.....	2
DESIGNATED SAFEGUARDING LEADS (DSLs)	2
TRUST IT TEAM / SCHOOL IT SUPPORT	2
STAFF	2
STUDENTS.....	2
PARENTS/CARERS	3
EQUALITY IMPACT ASSESSMENT (EIA)	3
RELEVANT LEGISLATION AND POLICIES.....	3
DEFINITIONS.....	3
UNACCEPTABLE USE FOR STAFF, STUDENTS, GOVERNORS, VOLUNTEERS AND CONTRACTORS.....	4
EXCEPTIONS TO UNACCEPTABLE USE.....	5
SANCTIONS.....	5
ARTIFICIAL INTELLIGENCE (AI).....	5
STAFF (INCLUDING GOVERNORS, VOLUNTEERS AND CONTRACTORS)	
6	
ACCESS TO TRUST IT FACILITIES AND MATERIALS	6
USE OF PHONES.....	6
EMAIL	6
MICROSOFT TEAMS	7
PERSONAL USE	7
REMOTE ACCESS	8
MONITORING AND FILTERING OF THE TRUST NETWORK AND USE OF IT FACILITIES.....	8
PASSWORDS.....	9
UNACCEPTABLE USE OF TRUST IT OUTSIDE OF SCHOOL.....	10
MULTIFACTOR AUTHENTICATION.....	11
STUDENTS	11

ACCESS TO IT FACILITIES	11
SEARCH AND DELETION.....	11
UNACCEPTABLE USE OF TRUST IT AND INTERNET OUTSIDE OF SCHOOL.....	13
MONITORING AND FILTERING OF THE TRUST NETWORK AND USE OF IT FACILITIES...	13
PASSWORDS.....	14
REMOTE ACCESS	15
PERSONAL USE	15
EMAIL.....	15
MICROSOFT TEAMS	15
PARENTS/CARERS	16
ACCESS TO IT FACILITIES AND MATERIALS	16
COMMUNICATING WITH OR ABOUT THE SCHOOL.....	16
COMMUNICATING WITH PARENTS/CARERS ABOUT STUDENT ACTIVITY	16
DATA SECURITY	16
SOFTWARE UPDATES, FIREWALLS AND ANTI-VIRUS SOFTWARE.....	17
DATA PROTECTION	17
BEST PRACTICE.....	17
ENCRYPTION	17
USE OF REMOVABLE STORAGE	17
CYBER SECURITY	17
BRING YOUR OWN DEVICE (BYOD).....	18
STAFF	18
STUDENTS.....	19
PARENTS/CARERS AND VISITORS	20
MONITORING AND REVIEW	20
APPENDIX 1: ACCEPTABLE USE AGREEMENT FOR STUDENTS.....	21
APPENDIX 2: ACCEPTABLE USE AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	22
APPENDIX 3: GLOSSARY OF CYBER SECURITY TERMINOLOGY	23

INTRODUCTION

- 1.1 Information Technology (IT) is an integral part of the way Bridge Academy Trust works, and is a critical resource for students, staff, governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the Trust. The IT resources and facilities the Trust uses could pose risks to data protection, online safety and safeguarding.
- 1.2 This policy aims to:
- a) Set guidelines and rules on the use of school ICT resources for staff, students, parents/carers and governors.
 - b) Establish clear expectations for the way all members of the school community engage with each other online.
 - c) Support the Trust's policies on data protection, online safety and safeguarding.
 - d) Prevent disruption that could occur to the Trust through the misuse, or attempted misuse, of IT systems.
 - e) Support the school in teaching students safe and effective internet and IT use.
- 1.3 Breaches of this policy may be dealt with under our disciplinary policy for staff and under the school's behaviour policy for students.

SCOPE

- 2.1 This policy covers all users of the Trust's IT facilities, including governors, staff, students, volunteers, contractors and visitors.

ROLES AND RESPONSIBILITIES

BOARD OF TRUSTEES

- 3.1 The Board of Trustees:
- a) Approves the IT Policy and ensures compliance with legal, safeguarding and DfE digital standards.

BRIDGE EXECUTIVE BOARD (BEB)

- 3.2 BEB:
- a) Oversees cyber security, filtering and monitoring arrangements.

CHIEF FINANCE & OPERATIONS OFFICER (CFOO)

- 3.3 The CFOO:
- a) Ensures the Trust's IT systems and resources are funded, effective and aligned to operational needs.

DIRECTOR OF IT

3.4 The Director of IT:

- a) Leads Trust-wide IT strategy, security, infrastructure and compliance.
- b) Manages access, monitoring, system changes.
- c) Oversees incident response, cyber security controls and software approval.

DATA PROTECTION OFFICER (DPO)

3.5 The DPO:

- a) Advises on data protection compliance and oversees breaches, SARs and DPIAs.
- b) Works with IT to assess risks and ensure secure handling of personal data.

HEADTEACHERS / HEADS OF SCHOOL

3.6 Headteachers/Heads of School:

- a) Ensure local compliance with this policy by staff and students.
- b) Support reporting of incidents, breaches and concerns.

DESIGNATED SAFEGUARDING LEADS (DSLs)

3.7 DSL's

- a) Lead on safeguarding issues involving IT, filtering alerts and online behaviour.
- b) Respond to incidents involving harmful or inappropriate online content.

TRUSTS IT TEAM / SCHOOL IT SUPPORT

3.8 Trust IT Team/School IT Support:

- a) Manages accounts, devices, filtering, monitoring and day-to-day technical support.
- b) Ensures systems are updated, secure and configured correctly.
- c) Assists with investigations into IT misuse and breaches.

STAFF

3.9 Staff:

- a) Use Trust IT responsibly and securely.
- b) Protect passwords, personal data and devices.
- c) Report incidents, suspicious activity or breaches immediately.
- d) Follow all related Trust policies (GDPR, Safeguarding, Code of Conduct).

STUDENTS

3.10 Students:

- a) Follow the Acceptable Use Agreement and use systems safely and responsibly.

- b) Report harmful or concerning content to staff.
- c) Keep login details secure.

PARENTS/CARERS

3.11 Parents/Carers:

- a) Support safe online behaviour for their child.
- b) Follow Trust guidelines when communicating online about the school.

EQUALITY IMPACT ASSESSMENT (EIA)

- 4.1 An Equality Impact Assessment has been completed for this policy which identified no significant negative impacts.

RELEVANT LEGISLATION AND POLICIES

- 5.1 This policy refers to, and complies with the following legislation and guidance:

- a) [Data Protection Act 2018, UK GDPR \(General Data Protection Regulation\)](#) and [the Trust GDPR policy](#)
- b) [DfE – Keeping Children Safe in Education](#), [Child Protection Policy](#)
- c) [Trust Records Management Policy](#)
- d) [Trust Staff Code of Conduct](#)
- e) [Trust Social Media Policy](#)
- f) [Computer Misuse Act 1990](#)
- g) [Human Rights Act 1998](#)
- h) [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)
- i) [Education Act 2011](#)
- j) [Freedom of Information Act 2000](#)
- k) [Education and Inspections Act 2006](#)
- l) [Searching, screening and confiscation: advice for schools 2022](#)
- m) [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)
- n) [Education and Training \(Welfare of Children\) Act 2021](#)
- o) [UK Council for Internet Safety](#)
- p) [Meeting digital and technology standards in schools and colleges](#)

DEFINITIONS

- 6.1 The following terms are used throughout this policy and are defined as follows:

- a) **IT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the trust's IT service.
- b) **Users:** anyone authorised by the school to use the school's IT facilities, including governors, staff, students, volunteers, contractors and visitors.
- c) **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user.
- d) **Authorised personnel:** employees authorised by the Trust to perform systems administration and/or monitoring of the ICT facilities.
- e) **Materials:** files and data created using the school's IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

UNACCEPTABLE USE FOR STAFF, STUDENTS, GOVERNORS, VOLUNTEERS AND CONTRACTORS

- 7.1 The following is considered unacceptable use of the Trust's IT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings ([see section on sanctions](#)):
- a) Using the Trust's IT facilities to breach intellectual property rights or copyright.
 - b) Using the Trust's IT facilities to bully or harass someone else, or to promote unlawful discrimination.
 - c) Breaching any of the Trust's policies or procedures.
 - d) Any illegal conduct, or statements which are deemed to be advocating illegal activity.
 - e) Online gambling, inappropriate advertising, phishing and/or financial scams.
 - f) Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful.
 - g) Consensual and non-consensual sharing of nude or semi-nude images and/or videos and/or livestreams.
 - h) Activity which defames or disparages the Trust or schools, or risks bringing the Trust/Schools into disrepute.
 - i) Sharing confidential information about the Trust/schools, its students, or other members of the community.
 - j) Connecting any device to the Trust's IT network without approval from the Trust IT team.
 - k) Setting up any software, applications or web services on the Trust's network without approval by the Trust IT team, or creating or using programme, tool or item of software designed to interfere with the functioning of the Trust's IT facilities, accounts or data.

- l) Gaining or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from the authorised personnel.
- m) Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the Trust's IT facilities.
- n) Causing intentional damage to the Trust's IT facilities.
- o) Removing, deleting or disposing of the Trust's IT equipment, systems, programmes or information without permission from the Trust IT team.
- p) Causing a data breach by accessing, modification, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation.
- q) Using inappropriate or offensive language.
- r) Promoting a private business, unless that business is directly related to the Trust.
- s) Using websites or mechanisms to bypass the Trust's filtering or monitoring systems.
- t) Engaging in content that is radicalised, extremist, racist, antisemitic or discriminatory in any other way.

7.2 This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The Headteacher/Head of School, IT Director and Data Protection Officer (DPO) will use their professional judgement to determine whether any act or behaviour on the list above is considered unacceptable use of the Trust's IT facilities.

EXCEPTIONS TO UNACCEPTABLE USE

8.1 Where the use of Trust IT facilities (on the school or trust premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the IT Team's discretion for example, a member of staff may be permitted to temporarily access a restricted website for research purposes related to safeguarding training or curriculum development, provided prior approval is obtained.

SANCTIONS

- 9.1 Staff who engage in any unacceptable activities listed above may face disciplinary action in line with the Trust's Discipline & Dismissal Policy.
- 9.2 Students who engage in any unacceptable activities listed above may face disciplinary action in with the school's behaviour policy.

ARTIFICIAL INTELLIGENCE (AI)

10.1 Refer to the AI Policy.

STAFF (INCLUDING GOVERNORS, VOLUNTEERS AND CONTRACTORS)

ACCESS TO TRUST IT FACILITIES AND MATERIALS

- 11.1 The Trust's IT Team manages access to the IT facilities and materials for Trust schools. That includes but is not limited to:
- a) Computers, tablets, mobile phones and other devices.
 - b) Access permissions for certain programmes or files.
- 11.2 Staff will be provided with a unique username and password that they must use when accessing the Trust's IT facilities.
- 11.3 Staff who have access to files that they are not authorised to view or edit, or who need their permissions updated or changed, should contact their schools IT team.

USE OF PHONES

- 11.4 The Trust records all external phone conversations.
- 11.5 Callers must be made aware that their phone call is being recorded. Incoming callers are notified of the recording in the menu messages that play.
- 11.6 All recorded calls are retained for 30 days before being automatically deleted. For more information, please see the Trusts Record Management Policy.
- 11.7 If staff wish to access a recorded phone call, they should contact the IT Team.
- 11.8 Staff must not give their personal phone number(s) to parents/carers or students. Staff must use phones provided by the Trust to conduct all work-related activities.
- 11.9 School phones must not be used for personal matters.
- 11.10 Staff who are provided with mobile phones as equipment for their role must abide by the same rules as set out in [Section 7](#).

EMAIL

- 11.11 The Trust provides each member of staff with an email address.
- 11.12 This Trust email account should be used for work purposes only.
- 11.13 Staff must not share their personal email addresses with parent/carers and students and must not send any work-related materials using their personal email account.

- 11.14 Staff must take care with the content of all emails, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- 11.15 Emails are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's mailbox does not mean that an email or Team's message cannot be recovered for the purposes of disclosure. All emails and Teams messages should be treated as potentially retrievable. All Trust emails are retained for 6 months before being automatically deleted from the email system. For more information, please see the Trust Records Management Policy.
- 11.16 Staff must take care when sending sensitive or confidential information by email. Any emails that contain sensitive or confidential information must be encrypted so that the information is only accessible by the intended recipient.
- 11.17 If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- 11.18 If staff send an email in error that contains personal information of another person, they must inform the Data Protection Officer immediately and follow the [data breach procedure](#). Staff should take care when opening attachments or clicking links in emails that are from an unknown sender, any concerns should be reported to IT Support.

MICROSOFT TEAMS

- 11.19 The Trust Teams account should be used for work purposes only.
- 11.20 Teams Messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents, Deletion from a user's mailbox does not mean that an email or Team's message cannot be recovered for the purposes of disclosure. All Teams messages should be treated as potentially retrievable. All Teams messages are retained for 30 days before being automatically deleted from the email system. For more information, please see the Trust Records Management Policy.
- 11.21 Staff must not have 1:1 Teams Calls or messages with students unless authorised by the School's Headteacher or Head of School. A risk assessment with the school's DSL must be conducted before any 1:1 sessions are started or scheduled.

PERSONAL USE

- 11.22 Staff are permitted to occasionally use Trust IT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The IT Director may withdraw or restrict this permission at any time and at their discretion.

11.23 Personal use if permitted provided that such use:

- a) Does not take place during teaching hours and non-break time.
- b) Does not constitute 'unacceptable use' as defined in [section 7](#).
- c) Does not interfere with their jobs, prevent other staff or students from using the facilities for work or education purposes.

11.24 Staff may not use the Trust IT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

11.25 Staff should be aware that use of the Trust's IT facilities for personal use may put personal communications within the scope of the Trust's IT monitoring activities ([see section 13.2](#)). Where breaches of this policy are found, disciplinary action may be taken.

11.26 Staff are also permitted to use their personal devices (such as laptops, mobile phones or tablets) in line with BYOD section. ([See section 16](#)).

11.27 Staff should be aware that personal use of IT facilities (even when not using Trust IT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where students and parents/carers could see them.

11.28 Staff should take care to follow the Trust's guidelines on use of social media and use of email and Teams to protect themselves online and avoid compromising their professional integrity.

REMOTE ACCESS

11.29 We allow staff to access the Trust's IT facilities and materials remotely. When using a Trust device, it will automatically dial in using a virtual private network (VPN).

11.30 Staff accessing the Trust's IT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the Trust's, IT facilities outside the Trust and must take such precautions as the IT team may require against importing viruses or compromising system security.

11.31 Our IT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our GDPR policy.

MONITORING AND FILTERING OF THE TRUST NETWORK AND USE OF IT FACILITIES

11.32 To safeguard and promote the welfare of staff and provide them with a safe environment to learn, the Trust reserves the right to filter and monitor the use of its IT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- a) Internet sites visited.
- b) Bandwidth usage.
- c) Email accounts.
- d) Teams accounts.

- e) Telephone calls.
- f) User activity/access logs.
- g) Any other electronic communications.

11.33 Only authorised IT personnel may filter, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

11.34 The Trust monitors IT use in order to:

- a) Obtain information related to Trust business.
- b) Investigate compliance with Trust policies, procedures and standards.
- c) Ensure effective IT operations.
- d) Conduct training and quality control exercises.
- e) Prevent or detect crime.
- f) Comply with a subject access request, Freedom of Information Act request, or any other obligation.

11.35 Our Governing board is responsible for making sure that:

- a) The Trust meets the DfE's filtering and monitoring standards.
- b) Appropriate filtering and monitoring systems are in place.
- c) Staff are aware of those systems and trained in their related roles and responsibilities.
- d) It regularly reviews the effectiveness of the Trust's filtering and monitoring systems.

11.36 The schools' designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

11.37 Where appropriate, staff may raise concerns about monitored activity with the Trust's DPO as appropriate.

PASSWORDS

11.38 All users of the Trust's IT facilities must set a strong password for their accounts and keep these passwords secure. Staff must set their password with 8 characters or more with a special character.

11.39 Staff can change their password by pressing CTRL+ALT+DELETE on their keyboard and clicking "Change a password".

- 11.40 Staff can also get their password reset by their school's IT Team if they are unable to remember their password. Passwords can be reset online using <https://passwordreset.microsoftonline.com/?whr=bridgeacademytrust.org> if they are offsite.
- 11.41 All users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.
- 11.42 Members of staff who disclose account or passwords information may face disciplinary action.
- 11.43 Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.
- 11.44 To help staff create a secure password, it is recommended that staff use three random words to create a secure password as recommended by the NCSC (National Cyber Security Centre). For more information, please see: <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words>.

UNACCEPTABLE USE OF TRUST IT OUTSIDE OF SCHOOL

- 11.45 The Trust will discipline staff, in line with the Trust's Discipline & Dismissal Policy, if a staff member engages in any of the following at any time (even if they are not on school premises):
- a) Using Trust IT to breach intellectual property rights or copyright.
 - b) Using Trust IT to bully or harass someone else, or to promote unlawful discrimination.
 - c) Breaching the school's/Trust's policies or procedures.
 - d) Any illegal conduct or making statements which are deemed to be advocating illegal activity.
 - e) Accessing, creating, storing, linking to or sending material; that is pornographic, offensive, obscene or otherwise inappropriate.
 - f) Consensual or non-consensual sharing of nudes and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery).
 - g) Activity which defames or disparages the Trust/school, other students, or risks bringing the Trust/school into disrepute.
 - h) Sharing confidential information about the Trust/school, other students, or other members of the school community.
 - i) Gaining or attempting to gain access to restricted areas of the network, or any password-protected information, without approval from the IT Team.
 - j) Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the Trusts IT facilities.
 - k) Causing intentional damage to the Trusts IT facilities or materials.
 - l) Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those share it with are not supposed to have access, or without authorisation.

- m) Using inappropriate or offensive language.

MULTIFACTOR AUTHENTICATION

11.46 All staff must use Multifactor authentication on all platforms that support it.

STUDENTS

ACCESS TO IT FACILITIES

- 12.1 Computers and equipment in the school's IT suites are available to students only under the supervision of staff.
- 12.2 Specialist IT equipment, such as used for music, design or technology, must only be used under the supervision of staff.
- 12.3 Students will be provided with an account to the Trust's Office 365 environment, which they can access from any device by using the following URL - <https://portal.office.com>

SEARCH AND DELETION

- 12.4 Under the Education Act 2011, the Headteacher, Head of School, and any member of staff authorised to do so by the Headteacher/Head of School, can search students and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:
 - a) Poses a risk to staff or students, and/or
 - b) Is identified in the school rules as a banned item for which a search can be carried out and/or
 - c) Is evidence in relation to an offence
- 12.5 This includes, but is not limited to:
 - a) Pornography.
 - b) Abusive messages, images or videos.
 - c) Indecent images of children.
 - d) Evidence of suspected criminal behaviour (such as threats of violence or assault).
- 12.6 Before any search, if the authorised member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
 - a) Make an assessment of how urgent the search is and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the Designated Safeguarding Lead or Headteacher/Head of School.
 - b) Explain to the student why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it.
 - c) Seek the student's co-operation.
- 12.7 The authorised staff member should:

- a) Inform the DSL (or deputy) if any searching incidents where they had reasonable grounds to suspect a student was in possession of a banned item.
 - b) Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk.
- 12.8 Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.
- 12.9 When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:
- a) Cause harm, and/or
 - b) Undermine the safe environment of the school or disrupt teaching, and/or
 - c) Commit an offence.
- 12.10 If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL/Headteacher or Head of School to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
- 12.11 When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:
- a) They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
 - b) Student and/or the parent refuses to delete the material themselves
- 12.12 If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:
- a) Not view the image
 - b) Not copy, print, share store or save the image.
 - c) Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- 12.13 Any searching of students will be conducted in line with:
- a) The DfE's latest guidance on searching, screening and confiscation.
 - b) UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

- c) The school's behaviour policy.

12.14 Any complaints about searching for, or deleting, inappropriate images or files on students' devices will be dealt with through the Trust's complaints procedure.

UNACCEPTABLE USE OF TRUST IT AND INTERNET OUTSIDE OF SCHOOL

12.15 The school will sanction students, in line with the school's behaviour policy, if a student engages in any of the following at any time (even if they are not on school premises):

- a) Using IT or the internet to breach intellectual property rights or copyright.
- b) Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination.
- c) Breaching the school's/Trust's policies or procedures.
- d) Any illegal conduct or making statements which are deemed to be advocating illegal activity.
- e) Accessing, creating, storing, linking to or sending material; that is pornographic, offensive, obscene or otherwise inappropriate.
- f) Consensual or non-consensual sharing of nudes and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery).
- g) Activity which defames or disparages the Trust/school, other students, or risks bringing the Trust/school into disrepute.
- h) Sharing confidential information about the Trust/school, other students, or other members of the school community.
- i) Gaining or attempting to gain access to restricted areas of the network, or any password-protected information, without approval from the IT Team.
- j) Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's IT facilities.
- k) Causing intentional damage to the school's IT facilities or materials.
- l) Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those share it with are not supposed to have access, or without authorisation.
- m) Using inappropriate or offensive language.

12.16 Any complaints about searching for, or deleting, inappropriate images or files on students' devices will be dealt with through the school complaints procedure.

MONITORING AND FILTERING OF THE TRUST NETWORK AND USE OF IT FACILITIES

12.17 To safeguard and promote the welfare of students and provide them with a safe environment to learn, the Trust reserves the right to filter and monitor the use of its IT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- a) Internet sites visited.
- b) Bandwidth usage.
- c) Email accounts.
- d) Teams accounts.
- e) Telephone calls.
- f) User activity/access logs.
- g) Any other electronic communications.

12.18 Only authorised IT personnel may filter, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

12.19 The Trust monitors IT use in order to:

- a) Obtain information related to Trust business.
- b) Investigate compliance with Trust policies, procedures and standards.
- c) Ensure effective IT operations.
- d) Conduct training and quality control exercises.
- e) Prevent or detect crime.
- f) Comply with a subject access request, Freedom of Information Act request, or any other obligation.

12.20 Our Governing board is responsible for making sure that:

- a) The Trust meets the DfE's filtering and monitoring standards.
- b) Appropriate filtering and monitoring systems are in place.
- c) Staff are aware of those systems and trained in their related roles and responsibilities.
- d) It regularly reviews the effectiveness of the Trust's filtering and monitoring systems.

12.21 The schools' designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

PASSWORDS

- 12.22 Secondary school aged students are required to set a password with a minimum of 6 characters, and it recommended that they have a special character. To help students create a password, it is recommended that students use three random words to create a secure password as recommended by the NCSC. For more information please see: <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words>.
- 12.23 If a student needs to change their password, they can visit their School's IT team or press CTRL+ALT+DELETE and click "Change a password".
- 12.24 Primary aged students are required to have a password with a minimum of 3 characters.

REMOTE ACCESS

- 12.25 We allow students to access the Trust's IT facilities and materials remotely. When using a Trust device, it will automatically dial in using a virtual private network (VPN).
- 12.26 Students accessing the Trust's IT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Students must be particularly vigilant if they use the Trust's, IT facilities outside the Trust and must take such precautions as the IT team may require against importing viruses or compromising system security.
- 12.27 Students must not provide parents/carers with access to Trust Office 365 accounts or Trust Devices.

PERSONAL USE

- 12.28 Students are permitted to occasionally use Trust IT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The IT Director may withdraw or restrict this permission at any time and at their discretion.
- 12.29 Personal use is permitted provided that such use:
- a) The Teacher has allowed the use of the IT facilities for personal use during lesson time.
 - b) Is during Break, Lunch, Before or after school.
 - c) Does not interfere with students from using the facilities for work or education purposes.
- 12.30 Students may not use the Trust IT facilities to store personal, non-school work-related information or materials (such as music, videos or photos).
- 12.31 Students should be aware that use of the Trust's IT facilities for personal use may put personal communications within the scope of the Trust's IT monitoring activities ([see section 12.17](#)). Where breaches of this policy are found, disciplinary action may be taken under the school's Behaviour policy.

EMAIL

- 12.32 The Trust provides each student with an email address.
- 12.33 Trust email account should be used for school purposes only.
- 12.34 All school-related work must be conducted using the email address the Trust/school has provided.
- 12.35 Students should take care when opening attachments or clicking link on emails that are from an unknown sender, any concerns should be reported to IT Support.

MICROSOFT TEAMS

- 12.36 Microsoft Teams must only be used for school related activities only.

ACCESS TO IT FACILITIES AND MATERIALS

13.1 Parents/Carers do not have access to the Trust's IT facilities.

However, parents/carers working for, the Trust in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the Trust's facilities at the Headteacher or Head of School's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to all staff.

COMMUNICATING WITH OR ABOUT THE SCHOOL

13.2 We believe it is important to model for students, and help them learn, how to communicate respectfully with and about others online.

13.3 Parents/carers play a vital role in helping model this behaviour of their child, especially when communicating with the Trust/school through our website and social media channels.

COMMUNICATING WITH PARENTS/CARERS ABOUT STUDENT ACTIVITY

13.4 The Trust/school will ensure that parents and carers are made aware of any online activity that their children are asked to carry out.

13.5 When we ask students to use websites or engage in online activities, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

13.6 In particular, staff will let parents/carers know which (if any) person or people from school students will be interacting with online, including the purpose of the interaction.

13.7 Parents/carers may seek any support and advice from the Trust/school to ensure a safe online environment is established for their child.

DATA SECURITY

14.1 The Trust is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and students. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cybercrime technologies.

14.2 Staff, students, parents/carers and others who use the Trust's IT facilities should always use safe computing practices. We aim to meet the cyber security standards recommended by the Department of Education's guidance on [digital and technology standards in schools and colleges](#), including the use of:

- a) Firewalls.
- b) Security features.

- c) User authentication and multi-factor authentication.
- d) Anti-malware software.

SOFTWARE UPDATES, FIREWALLS AND ANTI-VIRUS SOFTWARE

- 14.3 All of the Trust's IT devices that support software updates, security updates and anti-virus products will have these installed and be configured to perform such updates regularly or automatically.
- 14.4 Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the Trust's IT facilities.
- 14.5 Any personal devices using the Trust's network must all be configured in this way.

DATA PROTECTION

- 14.6 All personal data must be processed and stored in line with data protection regulations and the Trust's GDPR (Data protection) policy.
- 14.7 Users should not access, or attempt to access, systems, files or devices which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Data Protection Officer immediately.

BEST PRACTICE

- 14.8 Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out and shut down completely at the end of each working day.

ENCRYPTION

- 14.9 The Trust makes sure that it's devices and systems have an appropriate level of encryption.
- 14.10 Trust staff may only use personal devices to access Trust data, work remotely or take personal data (such as student information) out of school if they have been specifically authorised to do so.

USE OF REMOVABLE STORAGE

- 14.11 The Trust does not allow the use of removable storage such as portable hard drives or memory sticks. The Trust will only allow the use of removable storage in certain circumstances and approved by the Director of IT and Data Protection Officer.

CYBER SECURITY

- 15.1 Please see the glossary (appendix 3) to help with understanding cyber security terminology.

The Trust will:

- a) Work with governors and the Trust IT staff to make sure cyber security is given the time and resources it needs to make the Trust secure.

- b) Provide ongoing training for staff and students on the basics of cyber security.
- c) Make sure staff and students are aware of its procedures for reporting and responding to cyber security incidents.
- d) Investigate whether our IT software needs updating or replacing to be more secure.
- e) Not engage in ransom requests from ransomware attacks.
- f) Up to date with a system in place to monitor when the Trust needs to update its software.
- g) Regularly reviewed and tested to ensure that the systems are as effective and secure as possible.
- h) Backup critical data following the RPA 3-2-1 rules.
- i) Maintain the security of all IT Systems.
- j) Enable multi-factor authentication where systems and platform support this.
- k) Make sure Trust IT staff conduct regular access reviews to make sure each user in school/Trust has the right level of permission and admin rights.
- l) Have a firewall in place that is switched on and up to date, while also maintaining a rule log.
- m) Check that its supply chain is secure, for example by asking suppliers about how secure their business practices and are checking if they have the Cyber Essentials certification.
- n) Develop, review and test our Cyber Response plan with the IT team and other key stake holders.

BRING YOUR OWN DEVICE (BYOD)

16.1 The Trust's wireless internet connection is secure.

STAFF

16.2 Staff agree to the following before using the Wi-Fi:

- a) I agree that my device has the latest security updates installed, virus protection and firewall.
- b) Any personal device must be secured via a pin code or using a password and have all available security features on the device enabled before any connection to Trust systems including Wi-Fi.
- c) I agree that I will not share my username and password with others.
- d) The Trust/School is not responsible for any damages or loss, including personal files that may be deleted from the device.

- e) I agree that I am responsible for setting up my own equipment to access the BYOD network.
- f) I agree that I am responsible for the safety of device.
- g) I agree not to use a VPN (Virtual Private Network) or any other method to bypass the Trust's filtering system.
- h) I agree that use of the BYOD network is filtered and monitored by the Trust/school for safeguarding purposes.
- i) If a computer, smartphone or tablet is connected to the Trust's IT systems, or holds information belonging to the Trust, it is covered by the same rules for Acceptable Use as the Trust's own equipment regardless of who it belongs to.
- j) Personal IT devices may not be used in any way that is disruptive or not conducive to a positive working environment.
- k) The Trust has no responsibility for supporting any particular type of system. Technology changes and new types of devices may not be compatible with our services; any older devices may no longer be supported.
- l) The Trust reserves the right to withdraw access to its systems without notice.
- m) On leaving the Trust, data related to employment with us may be automatically deleted from the device.
- n) Cameras on personal devices must never be used to photograph or record students.

STUDENTS

- 16.3 Wi-Fi access is provided for free on "as in" with no guarantee of service. Wi-Fi networks may be subject to maintenance and downtime with no warning. The Trust reserves the right to revoke user access at any time. In certain schools only approved devices may use BYOD network.
- 16.4 If a student has a medical condition (such as diabetes) and need Wi-Fi access for a mobile device. If the medical app doesn't work, students are recommended to speak to the school's IT Team who will assist in unblocking the app. Students who have a medical condition and use the BYOD network are still subject to this policy.
- 16.5 Students agree to the following before using the Wi-Fi:
 - a) I agree that my device has the latest security updates installed, virus protection and firewall.
 - b) I agree that I will not share my username and password with others.
 - c) I agree that when asked to by a staff member that I will remove my device from the BYOD network immediately.
 - d) The Trust/School is not responsible for any damages or loss, including personal files that may be deleted from the device.
 - e) I agree that I'm responsible for setting up my own equipment to access the BYOD network.

- f) I agree that my device will be fully charged before bringing into school. Chargers are not available in school for personal devices.
- g) I agree that I'm responsible for the safety of device.
- h) I agree not to use a VPN (Virtual Private Network) or any other method to bypass the Trust's filtering system.
- i) I agree that use of the BYOD network is filtered and monitored by the Trust/school for safeguarding purposes.

PARENTS/CARERS AND VISITORS

- 16.6 Parents/carers and visitors to the school are not permitted to use the Trust's Wi-Fi unless specific authorisation is granted by the Headteacher or Head of School.
- 16.7 The Headteacher/Head of School will grant authorisation if:
 - a) Parents/carers are working with the school/Trust in an official capacity.
 - b) Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

MONITORING AND REVIEW

- 17.1 The Headteacher/Head of School, Director of IT and Data Protection Officer monitor the implementation of this policy, including ensuring it is updated to reflect the need and circumstances of the Trust.
- 17.2 This policy will be reviewed yearly.
- 17.3 This policy will be reviewed by the Data Protection Officer.

APPENDIX 1: ACCEPTABLE USE AGREEMENT FOR STUDENTS

Acceptable use of the Trust's IT facilities and internet: agreement for students and parents/carers

Name of student:

When using the Trust's IT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose!
- Use them without a teacher being present, or without a teacher's permission.
- Use them to break school rules.
- Access any inappropriate websites.
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms.
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- Use any inappropriate language when communicating online, including in emails.
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video.
- Share my password with others or log in to the school's network using someone else's details.
- Bully other people.

I understand that the school will monitor the websites I visit and my use of the school's IT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's IT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

I understand by signing this document I accept terms listed in the Trust/Schools IT Policy

Signed (student):

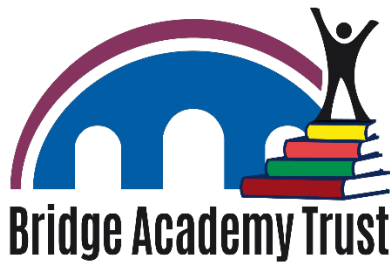
Date:

Parent/carers agreement: I agree that my child can use the Trust/school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the Trust/school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carers):

Date:

APPENDIX 2: ACCEPTABLE USE AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS



TO BE SIGNED AND RETURNED TO LINE MANAGER

(Failure to do so will result in loss of access to Trust IT Systems)

I agree that I have read the Trust IT Policy and agree to adhere to the contents within. If I have any questions, it is my responsibility to raise them with the Trusts IT team.

Location/School: _____

Name: _____

Signature: _____

Date: _____

APPENDIX 3: GLOSSARY OF CYBER SECURITY TERMINOLOGY

These key terms will help with understanding the common forms of cyber-attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) [glossary](#).

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where resources are stored and accessed (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt computer systems, networks or devices maliciously.
Cyber incident	Where the security of a system or service has been breached.
Cyber security	The protection of devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

TERM	DEFINITION
Pharming	An attack on computer network means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops the use of data or systems until a payment is made.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.