Acceptable Use Policy

Equalities Statement

In our Trust we work to ensure that there is equality of opportunity for all members of our community who hold a range of protected characteristics as defined by the Equality Act 2010, as well as having regard to other factors which have the potential to cause inequality, such as socio-economic factors.

Document Management	
Version Number:	V1.2
Date Approved:	January 2026
Next Review Date:	September 2026
Approved By:	Trust Senior Leadership Team
Responsible For:	Head of IT

Policy Revision Log	
Date	**Version No. Brief Detail of Change**
Sept 2025	V1.1 ● Added Password Requirements in Section 6.2 ● Added TheKeyGPT as approved AI in Section 7
Dec 2025	V1.2 ● Update section 7 with additional paragraphs for “Add to Drive” Gemini feature ● Update section 7 prohibiting staff and student data on personal AI systems ● Update section 4.3 updated to include the return of staff assigned equipment

Contents

1. Introduction and Aims

This policy applies to all users, whether on-site or off-site when:

- Using your Trust network account, including emails, on any device (including personal devices);
- Using Trust ICT equipment, including borrowed equipment;
- Representing a school or Trust.

This policy does not specify how users should use their personal devices (not school issued) or what they store on them, However, users should ensure personal files and software installed on their devices are isolated so as not to interfere with or contravene the Trust's policies. This is particularly important for those not directly employed by the Trust who could be working in areas outside of education where a different level of content may apply due to their employment.

Information and communications technology is an integral part of the way our schools work, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, the pastoral and administrative functions of everyone in the Trust.

However, the ICT resources and facilities our schools use could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of Trust IT resources for staff, pupils, parents and governors;
- Establish clear expectations for the way all members of the school community engage with each other online;
- Support the Trust's policies on data protection, online safety and safeguarding;
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems;
- Support the schools in teaching pupils safe and effective internet and ICT use.

This policy covers all users of the Trust's ICT facilities, including governors, staff, pupils, students, volunteers, contractors and visitors. The Acceptable use agreements can be found in the Appendix section.

2. Relevant Legislation and Guidance

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Unacceptable Use

The following is considered unacceptable use of the Trust's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings. Unacceptable use of the Trust's ICT facilities includes but is not limited to:

- Using the Trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination;
- Breaching the school's or Trust's policies or procedures;
- Any illegal conduct, or statements which are deemed to be advocating illegal activity;
- Gaming, gambling, inappropriate advertising, phishing and/or financial scams;
- Causing intentional damage to the Trust's ICT facilities;
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful;
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams;
- Activity which defames or disparages the institution, or risks bringing the institution into disrepute;
- Unauthorised sharing of confidential information about the school, its pupils, or other members of the school community;
- Connecting any device to the IT network without approval from authorised personnel;
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the Trust's ICT facilities, accounts or data;
- Gaining, or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel;
- Sharing your password with another member of staff, student or member of the public;
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the Trust's ICT facilities;
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel;
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation;
- Use of removal/portable storage devices (USB Sticks) not authorised in writing and for work purposes;

- Storing school data outside of swale.at Google Workspace solution, unless explicitly approved by the DPO and Head of IT;
- Photos or videos of pupils on personal devices;
- Photos or videos of staff on personal devices or chat systems without their permission;
- Entering personal data into AI system without permission;
- Using an AI system not linked to Swale account and approved by the DPO;
- Using the Trust's ICT facilities to breach intellectual property rights or copyright;
- Promoting a private business or referral system without approval;
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms;
- Engaging in content or conduct that is radicalised, extremist, racist or discriminatory in any other way.

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The Headteacher and/or IT Regional Manager will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the ICT facilities.

4. Staff

4.1 Multi Factor Authentication

As part of network and account security, Multifactor Authentication is enabled on all staff accounts, and should be completed as soon as possible after login details are provided.

Access to key systems and data will be restricted until Multi-factor Authentication setup has been completed.

Anyone who is unable to complete the multi-factor Authentication setup will need to speak to the school's IT Team as soon as possible, which may result in limited access to IT systems.

4.2 Use of Mobile Phones, email and Communication

The Trust provides each member of staff with an email address which should be used for work purposes only. All work-related business must be conducted using the email address the Trust has provided.

Users must take care with the content of all email messages, or chat messages as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email and chat 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 inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable. Users should not make inappropriate comments on email or chat.

Users must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information to 3rd parties must be encrypted so that the information

is only accessible by the intended recipient. Encrypted passwords must not be sent in the same email or a separate email to the same recipient of the email data without verifying via another method: e.g. phone or SMS.

Chat communication on Trust phones must be via Google Mail/Chat/Meet.

While personal phones can currently access work email, this could be removed at any time. Trust Email should only be used for professional work related communication. Sensitive information should only be accessed from work issued devices.

Users must not share their personal email addresses or phone number with parents or pupils and must not send any work related materials using their personal email or chat accounts.

4.3 ICT Hardware, portable devices and bookable resources

Staff will be provided with access to ICT hardware and other devices, including but not limited to desktop computers, laptops, tablets, mobile phones, desk phones, radios, interactive displays, printers and copiers depending on their role.

Where equipment is provided for the sole use of an individual, e.g. a teaching laptop or office desktop, it will be assigned directly to the named member of staff and logged in the school's asset registry.

Once assigned, the device and associated peripherals such as chargers, mice, keyboards and monitors, are the responsibility of the assigned individual, and any problems, loss or damage to the device or peripherals must be reported to the local IT Team as soon as possible, either in person or via helpdesk ticket.

Audit may request to see assigned devices as part of a regular asset and device check which must not be withheld. Staff can see which devices are assigned to them through the IT asset management system.

When not in use, devices must be kept secure, e.g. office doors locked, and portable devices (including laptops) placed somewhere secure (preferably lockable) and out of sight. When devices are left switched on and unattended, users must ensure they lock their screens. Any unattended devices found in an unsecured location should be removed and returned to the local IT team immediately.

Assigned devices (e.g. laptops) are provided to staff as a resource to be used as part of their job role. Where staff roles change, or for periods of prolonged absence (e.g. maternity, sickness, travel, sabbaticals) where staff are not expected to perform their role, the Trust reserves the right to request the return, and retain the use of these devices. An alternative device can be provided for the period of absence.

All staff issued devices must be returned to the local IT team in person on or before the end of the employment contract.

4.4 Responsibility and care for ICT equipment and shared resources

All staff have a responsibility to:

- Use ICT devices appropriately, for the intended work related purposes;
- Not damage, remove, modify or misplace any part or peripheral of the equipment;
- Report any missing or damaged items as soon as discovered.

The Trust/school reserves the right to claim the costs of repair or replacement to devices and peripherals from the assigned staff member or shared resource user. Any decision to claim costs is at the discretion of the Headteacher, Director of Primary and/or Director of Secondary.

4.5 Personal Use of Work Equipment

Staff are permitted to occasionally use ICT facilities for personal use, subject to certain conditions set out below. The Headteacher and/or IT Regional Manager may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/non-break time;
- Does not constitute 'unacceptable use';
- Takes place when no pupils are present;
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes.
- No additional software required
- No additional firewall or websites would need to be unblocked

Staff may not use the ICT facilities to store personal, non-work-related information or materials (for example music, videos or photos).

Staff should be aware that use of the ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities.

Staff should take care to follow the school's guidelines on use of social media (see the Social Media section of the Trust's E-Safety Policy) and use of email to protect themselves online and avoid compromising their professional integrity.

4.6 Filtering and Monitoring

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the Trust reserves the right to filter and monitor the use of its ICT facilities and network.

Only authorised IT Support and Safeguarding staff may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. DSLs have access to the web filtering system for both staff and students.

Where appropriate, authorised personnel may raise concerns about monitored activity with the DSLs and IT Regional Manager, as appropriate.

The effectiveness of any filtering and monitoring will be regularly reviewed.

5. Students

5.1 Access to ICT facilities

Pupils will be provided with their own unique, personal account which can be used to access the Trust computer systems, emails, and relevant learning platforms and resources. This account is the responsibility of the pupil, it should be kept secure and not shared with anyone else.

Pupils have access to the following ICT facilities during the school day and in some after-school activities:

- Computers and equipment in the school's ICT suite(s) and department ICT areas. Pupils should not enter any ICT suite without a supervising staff member.
- Some schools/departments may have devices that can be borrowed. These should be signed out and back in with a member of department staff, not just taken. Borrowed equipment should not be taken home or off site without express written permission from the school.
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff.
- Camera and portable video equipment for use in Media, Art or Photography courses. This should be signed out and back in with a member of department staff, not just taken. Borrowed equipment should not be taken home or off site without express written permission from the school.

Pupils may not use personal devices on the school network. Sixth-form pupils are given more freedom to use IT resources independently of staff supervision, for educational purposes only, but any abuse of this privilege will lead to sanctions and standard pupil restrictions being applied.

5.2 Responsibility and care for ICT equipment

All pupils have a responsibility to:

- Use ICT devices appropriately, for the intended work or learning related purposes.
- Not damage, remove, modify or misplace any part or peripheral of the equipment.
- Report any missing or damaged items as soon as discovered.

The Trust/school reserves the right to claim the costs of repair or replacement to devices and peripherals from any user proven to have caused loss or damage. Any decision to claim costs is at the discretion of the Headteacher.

6. Data Security

The Trust is responsible for making sure each school has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. 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 cyber-crime technologies.

Staff, pupils, parents and others who use the ICT facilities should use safe computing practices at all times. We are actively working towards the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls & Filtering;
- Security features;
- User authentication and multi-factor authentication;
- Anti-malware software.

6.1 Account Security

To ensure the security and integrity of the school's systems and protect the personal data of all users. All users of the ICT facilities should set strong passwords for their accounts and must keep these passwords secure and confidential.

Users are prohibited from sharing their accounts or passwords with anyone, including friends, family or staff members, including the IT staff.

Passwords for Swale online systems must not be the same as any password for any personal or online accounts.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Staff are required to set up Multi-Factor Authentication (aka 2FA) for their Swale.at google account.

Members of staff or pupils who disclose account or password information may face disciplinary action. Visitors or volunteers who disclose account or password information may have their access rights revoked.

6.2 Password Requirements

The password requirements for staff is as follows:

Minimum Length:	10 characters
Complexity:	Enforced Strong
Uniqueness:	Cannot be re-used
2FA:	Required

Strong password enforcement will check randomness of passwords, common passwords and known password breaches. This will block weak or exploited passwords from being set.

The password requirements for students is as follows:

Student Passwords	
Minimum Length:	8 characters
Complexity:	Standard
Uniqueness:	Cannot be re-used
2FA:	Not-required

Any password detected to be compromised will be reset.

6.3 Personal Devices

Personal devices must not connect to the Trust's main or guest networks and should not be used in school with some exceptions:

Staff may use personal devices such as computers, tablets and phones to access school data on Google remotely providing these devices have appropriate levels of security and meet DfE standards on security updates.

Staff are permitted to add a personal device to the schools dedicated 2FA network if available. Social media, 3rd party messaging systems or wifi calling will not be permitted. The Trust reserves the right to remove any personal device from the network at any time.

Personal devices can be used for 2FA authentication in line with the DfE guidance.

6.4 Access to resources

All users of the Trust's ICT facilities will have clearly defined access rights to school systems, files and devices.

Users should not access, or attempt to access, systems, files or devices to 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 local IT Support team immediately, either in person or via a helpdesk ticket.

Users should either lock or log out of systems or secure their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be secured at the end of each day.

6.5 Use of Public wifi

Staff should not use public wifi with work devices.

6.6 Removable Storage

In line with DfE security standards a block for staff on all removable storage devices (such as USB sticks, memory cards, portable hard drives, cameras, phones and tablets) when connected to Trust computers. This is to prevent unknown devices transmitting infected, malicious or prohibited files onto the Trust network and to prevent Trust data being stored on unmanaged devices.

Staff can request access for a removable storage device for specific work purposes (cameras, 3d printers) by submitting a helpdesk ticket and presenting the device to the local IT Support team.

Users must use Swale Google for file storage, rather than removable storage devices.

6.7 Third Party Applications (inc Cloud Services)

Any application/service requiring a user to login to consume its services should support SSO integration Google Apps for Education, to allow conditional access to be achieved.

We will need to remove solutions that require additional accounts to be created. Any application/service requiring student/staff data to be uploaded should be achieved by using WONDE or similar automatic data sync.

7. AI

Staff are permitted to use the Swale.at account linked Google Gemini, TheKeyGPT, NotebookLM and Bromcom AI tools. Staff can experiment with these tools for: drafting guidance; lesson and activity planning; generating quizzes; providing summaries; idea generation; and generating reason or comprehension activities.

Staff may use the "Add files from Google Drive" feature within Google Gemini to open existing Drive documents directly for planning, summarising and drafting.

Staff must not use Gemini with: safeguarding case files, individual SEND case files, detailed medical records, HR documents, or any other highly sensitive documents.

Staff are prohibited from entering staff or student personal or sensitive data into free or premium AI systems that do not have commercial data protection and are not linked to a work account. Staff must not use any personal AI account services on school devices. Staff must not use staff or student data on any personal AI system.

For additional AI services staff must complete a DPIA and where appropriate a IDTA. If the service is essential, seek consent before signing up themselves or asking others to sign up for websites using personal information for work or education purposes. Staff must respect the terms and conditions, including the age restriction of the sites, data storage locations and GDPR.

Staff are responsible when providing content output from an AI.

If AI service providers change their policy on the use of training data, introduce barriers to deleting content, remove security features or are purchased by another organisation, access may be removed without notice.

8. Subscription Services

Subscription services are contracts, staff must follow the Financial Regulations Policy.

9. Internet Access

If users are able to access a site hosting inappropriate content, they should submit a helpdesk ticket with the URL and other relevant details of the site. Pupils should report the incident to their class teacher. Attempts to deliberately access inappropriate or malicious sites, or circumvent the filtering system (e.g. via the use of proxy websites), will lead to sanctions being applied in line with the behaviour/disciplinary policy.

Some legitimate sites may be blocked if they have been categorised under a restricted category. Staff that require access to a blocked site for teaching or work purposes can submit a helpdesk ticket with details of the URL, the professional reason why it should be unblocked (the filter block page will provide this information), and whether the site is required for staff and/or pupil access. The IT Support Team will need to review the site's content to ensure it is safe/appropriate before it can be unblocked.

Each school provides passwordless wireless for staff issued devices and guest wireless networks.

- Users must not share or allow their network account details to be used by other people to access the internet;
- The Guest networks are time limited and for guests, not staff or students.

9.1 Guest Access

Guests to Trust schools are able to connect to the Trust Guest wireless network when required for specific, time limited, agreed purpose.

Staff devices should not be given to visitors to use as this may provide them inadvertently with unauthorised access to Trust data. Doing so could result in disciplinary action.

Where possible, staff should find out prior to the scheduled date whether or not their visitor(s) will require internet access to fulfil the purpose of their visit, and confirm with the Headteacher that it is acceptable for Guest network access to be granted.

Staff should not ask guests to provide documentation/presentations on a USB stick as these are prohibited on trust devices. Guests can bring their own IT technology and as required connect to the internet via the guest SSID. Guests are permitted to plug their own devices into TVs/Projectors as part of an approved activity.

Staff can request the Guest network password from the school reception or IT Support Team, but this should not be shared with guests until they are on site.

The Guest network password must not be shared with pupils. Guests should be made aware of this as well.

Guest network access is provided as a free, as-is service by the School, and visitors using the network on their personal devices do so at their own risk. Both access to and the functionality of the Guest network can be removed or changed as required by the School to maintain the security and efficiency of the primary wireless networks across the site.

10. Monitoring and Review

Headteachers, IT Regional Manager, and Trust Leadership monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school and Trust.

11. Related Policies

This policy should be read alongside the school's policies on:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Trust Data Protection Policy
- Online Safety Policy
- Records Management Policy and Retention Schedule
- Financial Regulations Policy

Appendix 1: Staff, Governors and Directors

Acceptable use of the Trust's ICT and the internet: Staff, Governors and Directors
Name:
Role:
Assigned Devices:
This Acceptable Use Agreement (AUA) outlines the acceptable and unacceptable uses of the Trust's Information and Communication Technology (ICT) facilities by staff members. This AUA ensures responsible use of technology, protects the Trust's ICT systems and data, and promotes a safe and secure environment for all users. By using these facilities, I agree to use them appropriately and adhere to this AUA. This AUA applies to all users, whether on-site or off-site, using the network at any time when: ● Using your Trust network account, including emails, on any device (including personal devices). ● Using Trust ICT equipment, including borrowed equipment. ● Representing a school or Trust. The policy is governed by the laws of England and by using a Swale Academies Trust account.
I have read, understood and agreed to the Acceptable Use Policy. I understand that the school will monitor the websites I visit and my use of the Trust's ICT facilities and systems. I will let the designated safeguarding lead (DSL) know if a pupil informs me that they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the Trust's ICT systems and internet responsibly and ensure that pupils in my care do so too. I will take responsibility for and care of any ICT equipment that is assigned to me directly, or resources that I book/loan for either my use or the use of pupils I am responsible for. I understand that I may be charged for any loss, damage or breakages to equipment that have been assigned to me.
School:
Signed:
Date:

Appendix 2: Pupils 11+

Acceptable use of the Trust's ICT facilities and the internet: agreement for students aged 11+

By logging on to, accessing or using any of the Trust's ICT facilities or accounts, you are automatically agreeing to and accepting the terms of this Acceptable Use Policy.

The Agreement

I understand that I must use school devices and systems in a responsible way and that this agreement will help keep me safe when I am online at home and at school.

This Acceptable Use Agreement is intended to ensure:

- that all pupils at the school/setting will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and the safety of those using them at risk. Pupils will have good access to digital technologies to enhance their learning and school/setting will, in return, expect the pupils to agree to be responsible users.

For my own personal safety:

- I understand that the school/setting will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of the risks of communicating with others online, and in particular those who I have only met online.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, where I go to school or information about my money)
- I understand the risks associated with meeting someone offline that I have only communicated with online and will not do this without speaking to a trusted adult.
- I will immediately report any unpleasant, offensive or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I understand that the school/setting internet filter is there to protect me, and I will not try to bypass it.
- I will make sure that my internet use is safe and legal, and I am aware that some online actions can have real life consequences.
- I know I must always check my privacy settings are safe and private.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school/setting and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not use the school/setting systems or devices for on-line gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me and:

- I will not access or change other people's files, accounts, or information.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I know that bullying in any form (on and offline) is not tolerated and I know that technology should not be used for harassment.

- I will not take or distribute images of anyone without their permission.
- I will write emails and online messages carefully and politely as I know they could be forwarded or seen by someone I did not intend.
- I understand that it may be a criminal offence or breach of the school/setting policy to download or share inappropriate pictures, videos, or other material online. I also understand that it is against the law to take, receive, save or send indecent images of anyone under the age of 18.
- I will always think before I post online. I know that text, photos or videos can become public and very difficult and sometimes impossible to delete.
- I understand that the school/setting has a responsibility to keep the technology it offers me safe and secure.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the email (due to the risk of the attachment containing viruses or other harmful programmes). Even if I know the sender, I will take care and not click on any links if something looks suspicious.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer/device settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- If using AI, I will do so within the rules agreed by my school.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school/setting also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community, e.g. if my behaviour online poses a threat or causes harm to another pupil and/or could have repercussions for the orderly running of the school then I understand that the school can take action against me.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action in line with the school's behaviour policy. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

School:
Name:
Signed:
Date:

Appendix 3: Pupils 7-11

Acceptable use of the Trust's ICT facilities and the internet: agreement for aged 7-11

By logging on to, accessing or using any of the Trust's ICT facilities or accounts, you are automatically agreeing to and accepting the terms of this Acceptable Use Policy.

The Agreement

I understand that I must use school devices and systems in a responsible way and that this agreement will help keep me safe when I am online at home and at school.

This Acceptable Use Agreement is intended to ensure:

that pupils at the school will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.

For my own personal safety:

- I know that I can use the internet in school and, to keep myself and others safe, I must use it responsibly.
- I will not share my password with anyone, and I will log off when I have finished using the computer or device.
- I will protect myself by not telling anyone I meet online any of my personal information. This includes my address, my telephone number, and my school's name.
- I will not send a picture of myself without permission from a teacher or other adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

I understand that everyone has equal rights to use technology as a resource and:

- I know that posting anonymous messages or pretending to be someone else is not allowed.
- I know that information on the internet may not be reliable and it sometimes needs checking so I will not download any material from the internet unless I have permission.
- I know that memory sticks/CDs from outside of the school may carry viruses so I will always give them to my teacher so they can be checked before opening them.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school.
- I know that the school internet filter is there to protect me.
- I know that all school accounts and systems are monitored, including when I am using them at home.

I will act responsibly towards others, as I expect others to act towards me and:

- I will be polite and sensible when I message people online
- I will not be rude or hurt someone's feelings online.
- I will not look for bad language, inappropriate images or violent or unsuitable games and, if I accidently come across any of these, I will report it to a teacher or adult in school or a parent/carer at home.
- If I get unkind, rude, or bullying emails or messages, I will report them to a teacher/adult. I will not delete them; I will show them to the adult.

School:

Name:

Appendix 3: Pupils under 7

Acceptable use of the Trust's ICT facilities and the internet: agreement for pupils aged under 7
By logging on to, accessing or using any of the Trust's ICT facilities or accounts, you are automatically agreeing to and accepting the terms of this Acceptable Use Policy.
Early Years and Key Stage 1 (0-6) **The Agreement** This Agreement is intended to help our younger pupils understand: ● How to stay safe while using the internet and other digital technologies for educational, personal and recreational use. ● That they must use school systems in a responsible way, to ensure that there is no risk to their own safety or to the safety and security of the systems and other users. This is how we stay safe when we use computers at school and at home: ● I will ask an adult if I want to use the computers / devices and will only use it when they are with me. ● I will only use activities that an adult has told or allowed me to use. ● I will keep information about me safe. ● I will not share my password. ● I will be kind to others online when I am sending messages. ● I will ask for help from an adult if I am not sure what to do or if I think I have made a mistake. ● I will tell an adult if I see something that upsets me on the screen or if I am worried. ● I know that if I break these rules, I might not be allowed to use the computers / devices. When I am learning from home: ● I will ask an adult if I want to use a computer or device. ● I will make sure that I use my computer or device in a sensible place (not in my bedroom). ● I will only do activities online that a teacher or suitable adult has told me or allowed me to use. ● I will ask for help from an adult if I am not sure what to do or if I think I have made a mistake. ● I will tell a teacher or adult if I see something that upsets me on the screen.
School:
Name: