ICT and Acceptable Use Policy (AUP)

Meridian Trust

Approved by:	Meridian Trust Finance & Resources Committee	**Date:** 22nd Sept 2025
Last reviewed on:	Sept 2025	
Next review due by:	Sept 2027	

Contents

1. Introduction and aims

Information and communications technology (ICT) 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 the school.

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 school ICT 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, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our behaviour policy or staff code of conduct.
Trust and individual school policies can be found via the links in Appendix 6.

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. Definitions

- **ICT 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 which may become available in the future which is provided as part of the Trust's ICT service
- **Users:** anyone authorised by the school to use the Trust's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the Trust to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the Trust's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs
- **Headteacher/Principal:** the head of the institution, can mean headteacher, principal, or anyone appointed to temporarily act in the role of head of the institution
- **IT Management Board:** the IT Directorate management team responsible for ICT across the trust
- **Trust/School:** the interchangeable word indicating the institution in all contexts

See appendix 7 for a glossary of cyber security terminology.

4. 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 (see section 4.3 below).

Unacceptable use of the Trust's ICT facilities includes:

- Using the Trust's ICT facilities to breach intellectual property rights or copyright
- Using the Trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school'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
- 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
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the ICT 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
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the Trust's ICT facilities
- Causing intentional damage 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)
- Storing school data outside of the Microsoft Office 365 solution, unless explicitly approved by the DPO and/or Director of IT
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic 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 Area 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.

Serious breaches or misconduct will be reported to the Executive Board and Directorate of the Trust.

4.1 Unacceptable use of ICT and the internet outside of school

This policy 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

This policy does not specify how users should use their personal devices 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.

Users will be sanctioned in line with the behaviour policy or staff code of conduct.

Please refer to section 4.2 above for details on sanctions and relevant behaviour policies.

4.2 Exceptions from unacceptable use

Where the use of the ICT facilities (on premise 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 Headteacher's discretion.

If you need to request an exemption, please contact the Headteacher of Trust Director of IT to ensure they are happy for the activity to go head. Once approved by the Headteacher, please submit a ticket to the IT Helpdesk ticket system **at least 4 weeks in advance of the activity**, with precise details including:

- The location, date and time the activity will take place
- Which ICT resources will be required for the activity
- Any specific software or web URL's that will be required for the activity
- Which age/year groups will be participating in the activity
- Any other details or requirements you think will be relevant to the activity, e.g: extra power, ports

The IT Team will review the request and let you know if it possible or not within 2 weeks of receiving the request. Any software or URL's that are not already in use across the Trust will need to be cleared by the DPO as part of the process.

4.3 Sanctions

Users who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's and Trust's policies.

Trust and individual school policies can be found via the links in Appendix 6.

5. Staff (including trustees and academy councillors)

5.1 Access to school ICT facilities and resources

The Trust's IT Team manage access to the ICT facilities and resources. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes, resources and data

Users will be provided with unique login(s)/account information and passwords that they must use when accessing the ICT facilities, resources and data.

Users who find they have access to data or files that they are not authorised to view or edit should report this to the IT Support Team as soon as possible, either in person or via the IT Helpdesk ticket system.

Staff who need their access permissions updated or changed should contact the school's local IT Support Team via the IT Helpdesk ticket system.
Requests for access to some resources, systems or data may need to be approved by the Headteacher, DSL or Trust Core IT Team.

Generic accounts are generally prohibited unless in explicit circumstances where data security can be maintained. This will be approved by the IT Directorate.

5.1.1 Multifactor Authentication (also referred to as MFA or 2FA)

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

Multifactor Authentication must be set up on a secure personal device/system that is not shared with any other person.

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

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

5.1.2 Use of phones and email

The Trust provides each member of staff with an email address which should be used for work purposes only.

All work-related business should be conducted using the email address the Trust has provided.

Users must not share their personal email addresses with parents or pupils and must not send any work-related materials using their personal email account.

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

Email 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 e-mail.

Users must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If users 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.

If users send an email in error that contains the personal information of another person, they must complete a 'reporting a data breach form' on https://www.meridiantrust.co.uk/key-information/gdpr/ This is reported automatically to the Data Protection Officer. If the form is not accessible, please inform the Trust's Data Protection Officer by email on DPO@meridiantrust.co.uk immediately and follow the Trust's data breach procedure.

Users must not give their personal phone number(s) to parents or pupils. Users must use phones provided by the Trust to conduct all work-related business.

Trust phones must not be used for personal matters.

Users who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

It is possible for users to record calls made or received through Microsoft Teams. Users intending to record a call need to make other callers aware that the call will be recorded at the start of the call.
Users may wish to make other callers aware at the start of the conversation that calls can be recorded, in case it becomes necessary to initiate a recording during the conversation, even if it was not planned to record the conversation initially.

5.2 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 as part of 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 should be reported to the local IT Support Team as soon as possible, either in person or via helpdesk ticket.

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

When devices are left switched on and unattended, users must ensure they lock their screens (⊞ & L).

When not in use, devices should be kept secure, e.g. office doors locked, and portable devices (including laptops) placed somewhere secure (preferably lockable) and out of sight. Devices taken off site must be covered under your home or vehicle insurance. Any unattended devices found in an unsecured location should be removed and returned to the local IT Support 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/paternity leave, 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.

5.2.1 Shared and bookable ICT resources

Schools also provide access to shared and bookable resources such as ICT suites and trolleys of laptops or tablets. These are booked out to a single named individual, e.g. the class teacher, **and are the responsibility of that individual for the duration of the booking.**

Where possible, staff should make a seating plan for ICT suites to identify which pupils are using each device.

At the beginning of the session, the member of staff in charge of the lesson must check the condition of each device (or ask pupils to identify any missing or broken equipment) and report any problems to the local IT Support team via a helpdesk ticket before the end of the lesson.

The member of staff in charge of the lesson should also perform a brief visual check at the end of each session to ensure nothing has been broken or misplaced during the session, and report any missing or broken equipment to the local IT Support team via a helpdesk ticket, with the name(s) of pupils that were using that equipment.

Staff have the ability to monitor the activity of all networked devices. Student devices may be monitored by the teacher during a lesson using Classroom.Cloud.

Any misbehaviour or damage to ICT equipment should be dealt with under the school's behaviour policy.

5.2.2 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 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 or Executive Board member.

5.3 Requesting new software or cloud services

Staff may want or need to request new software or cloud-based services in addition to the programs and services already provided by the Trust or school.

Any new software or cloud service requested for either work or teaching and learning must go through a process of investigation by both the Trust DPO and IT Team to ensure it is safe, secure, appropriate, value for money, and in compliance with GDPR and other relevant policies. The request may need to go via the Trust's curriculum director if used in multiple schools.

Any software or service that does not meet all of the requirements will be rejected.

Any requests for new software or cloud services should be submitted to the IT Team via a helpdesk ticket (IT@meridiantrust.co.uk). The IT Team will submit the request to the DPO as part of the investigation process.

Staff should allow at least 21 days for the investigation process.

5.4 Personal use

Staff are permitted to occasionally use ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Headteacher and/or IT Area 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', as defined in section 4
- 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

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 (see section 5.7). Where breaches of this policy are found, disciplinary action may be taken.

Staff are permitted to use their personal devices (such as mobile phones or tablets) in line with the e-safety and KCSIE guidelines and where applicable a school's mobile phone policy.

Staff should be aware that personal use of ICT (even when not using the ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them, or bringing the institution into disrepute.

Staff are reminded about the licencing restrictions of using "personal" subscriptions outside of the home. Many of the streaming platforms (including Spotify) explicitly state it is for personal use only and not commercial or educational use. Schools cannot purchase Spotify personal accounts to use within the school environment.

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 - https://www.meridiantrust.co.uk/key-information/policies/ and use of email (see section 5.1.2) to protect themselves online and avoid compromising their professional integrity.

5.4.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

See the Social Media section of the Trust's E-Safety Policy - https://www.meridiantrust.co.uk/key-information/policies/

5.5 Remote access

While most of the School and Trust's data and resources are available at all times through Teams, OneDrive and Office 365, some key systems are only available while on network (SIMS, PSF Financials).
The Trust allows specific staff to access these resources remotely via a secure remote desktop solution or VPN.

Staff accessing the ICT 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 ICT facilities outside the school and take such precautions as the Trust's IT Support Team may require against importing viruses or compromising system security.

The Trust's ICT 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 the Trust's data protection policy.

The Trust's Data Protection policy can be found on the Trust's Policies page:
https://www.meridiantrust.co.uk/key-information/policies

5.6 School social media accounts

Trust schools may have official social media accounts, managed by designated users. Users who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The IT Area Manager must have access to all school social media accounts, either by having a separate administrator login, or being given the username and password if only one administrator account exists.

The Trust has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.7 Monitoring and filtering of the school network and use of ICT facilities

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. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs and keystrokes
- Any traffic which has passed through the Trust's network
- Any other electronic communications

Only authorised IT Support and Safeguarding staff may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

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

Where appropriate, authorised personnel may raise concerns about monitored activity with the school's designated safeguarding lead (DSL) and IT Area Manager, as appropriate.

The Trust monitors ICT use in order to:

- Obtain information related to school operations
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operations
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation, as detailed in the GDPR Privacy Policy

The Trust will regularly review the effectiveness of the school's monitoring and filtering systems.

6. Pupils

6.1 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.
  This 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.

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.

6.1.1 Responsibility and care for ICT equipment and shared resources

All pupils have a responsibility to:

- Use ICT devices appropriately, for the intended work or learning related purposes.
- Not damage, remove 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 cause loss or damage. Any decision to claim costs is at the discretion of the Headteacher.

6.2 Search and deletion

Under the DFE's Searching, Screening and Confiscation 2022 guidance (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091132/Searching__Screening_and_Confiscation_guidance_July_2022.pdf), the Headteacher, and any member of staff authorised to do so by the Headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will act in compliance with the school's behaviour policy.

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.

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, or could be used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence
- Undermine or affect the safety and/or security of the Trust's computer or network systems

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL, Headteacher or other member of the Senior Leadership Team 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.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if 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 reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may deal with the data in line with the safeguarding and behaviour policies.

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

6.3 Canva

Canva users generally need to be 13 years or older, though students under 13 can use Canva for Education with teacher supervision and parental consent. This age restriction is in place because Canva allows for easy sharing of designs on social media, and the platform wants to ensure users are old enough to understand the implications of online sharing.

Individual schools will gain permission from a parent or guardian for students to use Canva.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the Trust's ICT facilities as a matter of course.

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

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

7.2 Communicating with or about the school online

We believe it is important to set an example for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

Where a school has an official channel for parents to communicate directly, we ask parents to read the expectations in appendix 2.

8. 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 aim to meet 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
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the ICT facilities should set strong passwords for their accounts and keep these passwords secure.

The Trust's password security policy is currently:

- Enforced change every 180 days
- Minimum length of 7 characters
- Minimum complexity requirements. Passwords cannot contain your name or username, and must have a combination of at least 3 of the following:
    - Upper case letters
    - Lower case letters
    - Numbers
    - Non-alphabetic symbols (e.g. ! @ £ $ # *)
- Password history of 10 passwords (how many new, unique passwords must be used before an old password can be used again)

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

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

8.2 Software updates, firewalls and anti-virus software

All of the Trust's ICT 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.

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 ICT facilities.

Personal devices cannot connect to the Trust's network, but can use the BYOD or Guest network Wi-Fi provided at all sites.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the Trust's data protection policy.

The Trust's Data Protection policy can be found on the trust's website – www.meridiantrust.co.uk/policies

For individual school's policy pages, please see Appendix 6

8.4 Access to ICT facilities and resources

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

These access rights are managed by the IT Area Manager for the school, and Trust central IT team.

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.

8.5 Encryption

The Trust makes sure that its devices and systems have an appropriate level of encryption.

Staff may use personal devices such as computers, tablets and phones to access school data on Outlook, Teams, OneDrive and Remote Desktop services (e.g. SIMS, PSF) remotely providing these devices have appropriate levels of security and protection.

Staff should be very cautious when using Trust devices or accessing any Trust data when using free/open/unsecured public connections, e.g. café or airport Wi-Fi provision.

8.6 Microsoft 365 Profile Pictures

Staff and Students pictures from the schools MIS and staff management software will be automatically extracted and placed as a profile picture in Microsoft 365. This cannot be removed as it uses an automated process and is used to safeguard all users.

9. Protection from cyber attacks

Please see the glossary (appendix 8) to help you understand cyber security terminology.

The Trust will:

- Work with the Academy Councils, School SLTs and IT Support Teams to make sure cyber security is given the time and resources it needs to make systems as secure as possible
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security.
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Ensure that ICT facilities are up to date and within their support and update lifetime. Out of date and insecure software will be removed, and hardware updated or replaced.
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **Proportionate**: The Trust will verify this using a third-party audit annually, to objectively test that what it has in place is effective
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data regularly.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the school's Data Managers
- Make sure staff use multi-factor authentication.
- Make sure staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall and filtering solution in place
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT Support department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested regularly.

9.1 Removable storage

As an additional protection against cyber attacks and malware, the Trust has implemented a block 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.

Staff can request access for a removable storage device by submitting a helpdesk ticket and presenting the device to the local IT Support team for a comprehensive virus scan. If any infected or malicious files or programs are found on the device, access will be denied.

Users are encouraged to use Teams and OneDrive for file storage, rather than removable storage devices, as these systems are more secure and can be accessed anywhere, on any device, as long as a network connection is available.

9.2 3rd Party applications (inc: Cloud services)

Any application/service requiring a user to login to consume its services must support SSO integration with Microsoft Azure or Google Apps for Education, to allow conditional access to be achieved.
The trust is actively removing solutions that require additional accounts to be created.

Any application/service requiring student/staff data to be uploaded must be achieved by using WONDE or similar automatic data sync. Applications which require a CSV upload will not be approved.
The trust is actively removing solutions that require a manual import/export of data.

Applications that do not confirm to the above will be gradually retired from use before September 2024.
See section 5.3.

9.3 Conditional Access Policy for Staff Accounts

To enhance the security of our systems, all staff accounts accessed outside of the school's network must be secured with Multi-Factor Authentication (MFA). This measure is to prevent unauthorized access to accounts by third parties. Approved MFA methods include:

- SMS text message to a personal phone
- Microsoft Authenticator application

These methods are non-invasive and, once set up, will only be required when accessing files and emails outside of the school's internet connection. Additionally, any access from outside the UK will be prohibited by default. This restriction can be lifted when staff inform IT that they are leaving the country for a set period of time.

Any staff account that cannot meet the above requirements will be restricted so that the account can only be accessed within the school's network

10. Internet access

Each site has a secure internet connection accessible via both wired and wireless connections. The Trust uses a filtering system to protect users and devices from inappropriate content and potentially malicious sites. This protection is extended to anywhere a Trust device is used, e.g. laptops at home.

Filtering systems are not fool proof and while every effort is made to monitor and update the filters to include new sites and threats, it is not possible to protect against all inappropriate or malicious content, especially if these are encrypted.

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 also 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, why it is blocked (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 sites content to ensure it is safe/appropriate before it can be unblocked.

Each school provides separate staff/pupil, BYOD (Bring Your Own Device) and guest wireless networks.

- BYOD networks require a Trust network account to access and are subject to the same filtering and restrictions as the main wired and wireless connection.
- Users must not share or allow their network account details to be used by other people to access the internet.
- The BYOD network is provided to allow staff and pupils to access the internet on personal devices, e.g. mobile phones, when access to an IT suite or laptop is not possible.
- The BYOD network should not be used for personal/non-work/non-educational purposes.

- Guest network access is password controlled. See Section 10.2 for further details.
- The Guest network password must not be shared with pupils.
- The Guest network password is changed by the Trust on a regular basis.

10.1 Pupils

Pupils may use the internet for any work or educational purpose as required for their lessons or studies, when permitted by a staff member. Any inappropriate, non-work/non-educational use will result in sanctions being applied as per the school Behaviour Policy, and internet privileges being restricted or revoked.

Pupils may, where permitted by the school, access the BYOD wireless network on their personal devices using their Trust network account, however this should only be done when such devices are allowed to be used by a member of staff as part of lessons/school work, and in line with the Trust's/school's Mobile Phone policy.

The BYOD network is filtered and sometimes bandwidth restricted to ensure equitable access.

Personal devices with inappropriate names that cause any disruption or issues that affect other users of the Trust network, will be blocked using the devices unique hardware ID, and prevented from accessing the Trust network in the future.

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

The BYOD network should not be used to circumvent the Trust's security and filtering systems. The use of legal and illegal VPN solutions is prohibited.

10.2 Parents and visitors

Parents and other visitors to Trust schools are able to connect to the Trust Guest wireless network.
A limited number of devices are available from the local IT Support team if required (e.g. interviews).

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 OK 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. Guest 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 Trust/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 Trust/school to maintain the security and efficiency of the primary Wireless networks across the site.

11. Monitoring and review

The Headteacher, IT Area 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.

This policy will be reviewed every 2-3 years.

12. Related policies

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

- E-safety
- Social media
- Safeguarding and child protection
- Behaviour
- Staff Code of Conduct
- Data protection (GDPR and Cyber-security)
- Remote education
- Mobile phone
- Governance code of conduct
- Records Management Policy and Retention Schedule
- All Trust and school policies are available via the Policy Portal: www.meridiantrust.co.uk/policies

Appendix 1: What to do if …

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to 1 parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
  - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents. Speak with your school's DSL
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: expectations for parents and carers

Acceptable use of the internet: expectations for parents and carers

Online channels are an important way for parents/carers to communicate with, or about, Trust schools.

Trust schools may use the following channels:

- Official Social Media pages (e.g. Facebook, Instagram, Twitter)
- Email/text groups for parents (for school announcements and information)
- Virtual learning platform

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's school or class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school or Trust via official communication channels, or using private/independent channels to talk about the school, we ask all parents/carers to:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

We also ask parents/carers not to:

- Use private groups, the school's Social Media pages, or personal social media to complain about or criticise members of staff. This is not constructive, and the school can't improve or address issues unless they are raised in an appropriate way
- Use private groups, the school's Social Media pages, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. Parents/carers should contact the school and speak to an appropriate member of staff about specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than their own, unless they have the permission of the other children's parents/carers

Appendix 3: Acceptable use agreement for pupils aged 11+

Acceptable use of the Trust's ICT facilities and internet: expectations for older pupils

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.

When using the Trust's ICT facilities and accessing the internet in school, I will:

- Use them for educational and schoolwork purposes only
- Use them only with a staff member present, or with a staff member's permission
- Use them responsibly and in line with school rules and this Acceptable Use Policy
- Be sensible in my use of the internet and not attempt to access inappropriate or malicious websites
- Not access social networking sites, unless my teacher has expressly allowed this as part of a learning activity
- Not bring in or attempt to access any inappropriate or malicious content on removable storage, remote storage (e.g. OneDrive) or personal devices
- Not use chat rooms, or use class Team chat inappropriately
- Be academically honest and will not use AI (Artificial Intelligence) tools for any part of my work, unless my teacher has allowed this as part of a learning activity
- Not open any attachments or follow any links in emails, without first checking with a teacher
- Not use any inappropriate language when communicating online, including in emails
- Never 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
- Never share my password with others or log in to the school's network using someone else's details
- Never bully other people

I understand that the school will monitor my activity on the network, which includes what sites I visit on the internet.

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, or pose a risk to the security of the Trust network or ICT facilities.

I will always use the school's ICT 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 that the school can charge me or my parents/carers for any loss, breakages or damage I cause to the school's ICT equipment.

Appendix 4: Acceptable use agreement for pupils aged under 11

Acceptable use of the Trust's ICT facilities and internet: expectations for younger pupils

By using a school computer or tablet, or your account, you are automatically agreeing to and accepting the terms of this Acceptable Use Policy.

When I use the Trust's ICT facilities (like computers and equipment) and go on the internet in school, I will:

- Ask a teacher first, and always make sure there is a staff member in the room with me
- Use them responsibly and following school rules
- Be sensible on the internet and only go to websites my teachers tell me to go on
- Not use social networking sites (unless my teacher said I could as part of a lesson)
- Not go on chat rooms, or be silly on class Team chats
- Ask my teacher first before opening any attachments or clicking links in emails
- Be nice to people, and not use mean or rude words when talking to other people online or in emails
- Never send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- Never tell my password to others, even my friends, or log in using someone else's name or password
- Never bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the Trust's ICT systems and internet.

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 that my parents/carers may have to pay to fix or replace equipment if I break, damage or lose it.

Appendix 5: Acceptable use agreement for staff, trustees and academy councillors

Acceptable use of the Trust's ICT facilities and the internet: agreement for staff, trustees and academy councillors

Name: _____.

Role: _____.

Assigned device asset (where applicable): _____.

When using the Trust's ICT facilities and accessing the internet in school, or outside school on a work device or account, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the Trust or school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the IT network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

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) and IT Area Manager 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 all reasonable steps to ensure that work devices are secure and password-protected when transporting or using them outside school, and keep all data securely stored in accordance with this policy and the Trust's data protection policy.

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.

Signed:	**Date:**

Appendix 6: Trust School website policy section links

Most policies at Meridian Trust are developed and approved centrally, but some polices such as Behaviour, Admissions, and Uniform are delegated to schools. Many centralised policies are published on the trust website on https://www.meridiantrust.co.uk/key-information/policies/

Policies delegated to the schools are on the school website pages listed in the table below. Each school page should also provide a link to the Trust's central policy page and should not duplicate policies contained therein with the exception of Safeguarding and Child Protection Policy which will be on both school and Meridian Trust websites.

Staff, Trustees and Academy Council members can also access all policies on the policies hub - https://cmat.sharepoint.com/sites/PoliciesHub

If you are not able to access a policy you need, please contact the school via the contact page or the trust via enquiries@meridiantrust.co.uk

Bar Hill Primary	https://www.barhillprimary.org/ofsted-policies
Downham Feoffees Primary	https://www.downhamfeoffees.org/policies/
Ely College and Bishop Laney 6th Form	https://www.elycollege.com/page/?title=Policies&pid=15
Great Ouse Primary	https://www.greatouse.beds.sch.uk/the-school/gopa-policies/
Greater Peterborough UTC	https://gputc.org/about-us/policies/
Harrold Primary Academy	https://www.harrold.beds.sch.uk/about-us/policies/
Hatton Park Primary	https://www.hattonpark.org/policies/
Histon and Impington Brook Primary	https://www.brookprimary.co.uk/policies/
Histon and Impington Park Primary	https://www.parkprimary.co.uk/policies/
Lincroft Academy	https://lincroft.academy/about-us/policies-statutory-information/
Martin Bacon Academy	https://www.martinbacon.academy/school-information/our-policies-and-procedures/
Nene Park Academy	https://www.neneparkacademy.org/policies-guidelines/
Nene Gate School	https://www.nenegateschool.co.uk/school-policies.html
North Cambridge Academy	https://northcambridgeacademy.org/policies/
Northstowe Secondary College	https://www.northstowesc.org/about/policies-statutory-information/
Oakley Primary Academy	https://www.oakley.beds.sch.uk/our-school/policies/
Sawtry Junior Academy	https://www.sawtryjunior.org/policies/
Sawtry Village Academy	https://www.sawtryva.org/academy-information/policies/
Sharnbrook Academy	https://sharnbrook.academy/academy-information/policies-and-protocols/
Somersham Primary School	https://www.somershamprimary.co.uk/policies/
Stamford Welland Academy	https://www.stamfordwellandacademy.org/policies/
Stratton Upper School	https://stratton.beds.sch.uk/index.php/key-information/policies
Swavesey Village College	https://www.swaveseyvc.co.uk/policies/
The Bluecoat School	https://bluecoatprimary.org/information/policies/
The Ferrers School	https://www.theferrers.org/policies/
The Harbour School	https://theharbour.academy/key-information/policies/
The Lantern Primary	https://www.lanternprimary.org/policies/
Trumpington Park Primary	https://www.trumpingtonpark.org/policies/
Weldon Village Academy	https://www.weldonva.org/policies/
West Town Primary	https://www.westtownprimary.org/policies/

Appendix 7: Glossary of cyber security terminology

These key terms will help you to understand 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 your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your 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.
Pharming	An attack on your computer network that 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 you from using your

TERM	DEFINITION
	data or systems until you make a payment.
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.