Aspire
Educational Trust

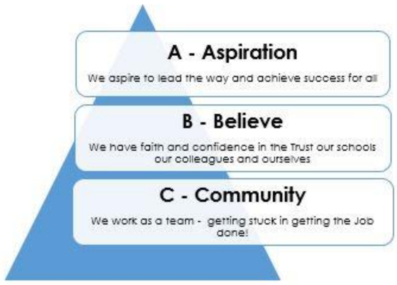
ICT and Electronic Devices Policy

Prepared by:	Shared with schools:
L.Treadway	**Summer 24**

Contents:

Statement of intent

All AET policies are written to support our schools and communities. We do this by ensuring they are always in line with our Colleague Values:


A - Aspiration
We aspire to lead the way and achieve success for all
B - Believe
We have faith and confidence in the Trust our schools our colleagues and ourselves
C - Community
We work as a team - getting stuck in getting the Job done!

Applying these values to everything we do means always acting with integrity, in the interests of others, being honest, open and transparent and putting the safety of our children first.

The Aspire Educational Trust believes that ICT plays an important part in both teaching and learning over a range of subjects, and the trust accepts that both trust/school-owned and personal electronic devices are widely used by members of staff. The trust is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

The trust has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

- Members of staff are responsible users and remain safe while using the internet.
- The Trust and its academies ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- Members of staff are protected from potential risks in their everyday use of electronic devices.

Personal use of ICT equipment and personal devices may be permitted; however, if authorised, this is strictly regulated and must be done in accordance with this policy, the Trust’s Cyber Security Policy, Social Media Policy and Online Safety Policy.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Freedom of Information Policy
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Online Safety Policy
- Photography and Images Policy
- Cyber-security Policy
- Records Management Policy
- Staff Code of Conduct

2. Roles and responsibilities

The Board of Trustees has the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

The principal is responsible for:

- The day-to-day implementation and management of the policy.
- The overall allocation and provision of resources within their academy.
- Handling complaints regarding this policy as outlined in the trust's Complaints Procedures Policy.
- Informing staff that the trust and the school reserve the right to access personal devices for the purpose of ensuring the effectiveness of this policy.
- Ensuring there is a system in place for monitoring internet activity of all users' accounts.
- Ensuring members of staff are allocated and complete AET required training for data protection, UK GDPR and cyber security.

The ICT technician is responsible for:

- Supporting the principal with their monitoring of internet activity of all user accounts and to report any inappropriate use identified to the principal.
- Remotely viewing or interacting with any of the computers on the school's network. This may be done randomly to implement this policy and to assist in any difficulties.

- Ensuring routine maintenance and security checks are carried out on school-owned and personal devices that are used for work purposes to check that appropriate security measures and software have been updated and installed.
- Ensuring that, though appropriate steps will be taken to ensure personal information is not seen during security checks, staff are made aware of the potential risks.
- Accessing files and data to solve problems for a user, with their authorisation.
- Ensuring the school's networks, configuration and security are aligned to the guidance given in the Cyber Security Policy.
- On the instruction of the principal, adjusting access rights and security privileges in the interest of the protection of the school's data, information, network and computers.
- On the instruction of the principal, disabling user accounts of staff who do not follow this policy and the accounts of employees that leave the organisation.
- Assisting the principal in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy.
- Assisting staff with authorised use of the ICT facilities and devices, if required.
- Immediately reporting any breach of devices to the principal or DPO.

The DPO is responsible for:

- Reviewing and amending this policy taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- Monitoring that trust or school-owned and personal electronic devices, authorised for work use, have security software installed, to protect sensitive data in cases of loss or theft.
- Monitoring that trust or school-owned devices are secured and encrypted in line with the trust's Data Protection Policy.
- Monitoring that all devices connected to the trust or its academies' networks and internet are encrypted.
- Monitoring all staff are aware of, and comply with, the data protection principles outlined in the trust's Data Protection Policy.
- Monitoring completion of required training for data protection, UK GDPR and cyber security.

Staff members are responsible for:

- Requesting permission from the principal, subject to their approval, before using school-owned devices for personal reasons during school hours.
- Requesting permission to loan school equipment and devices from the principal.
- Requesting permission from the principal, subject to their approval, before using personal devices during school hours and ensuring these devices are submitted for security checks when requested.
- Ensuring any personal devices that are connected to the trust and its academies' networks are in accordance with the trust's Cyber Security Policy.
- Undertaking required AET training for data protection and UK GDPR and cyber security.
- Ensuring security updates on the school/trust owned devices they are allocated are installed promptly and seeking support from the IT technician, if needed, to achieve this.

- Reporting misuse of ICT facilities or devices, by staff or pupils, to the principal.
- Reading and confirming as read the AET technology acceptable use agreement to confirm they understand their responsibilities and what is expected of them when they use school-owned and personal devices.

The IT Lead in each academy is responsible for the maintenance and day-to-day management of the equipment, as well as the device loans process.

The SBM/Bursar in each academy is responsible for:

- Maintaining a Fixed Asset Register to record and monitor the academy's assets.
- Ensuring value for money is secured when purchasing electronic devices.
- Monitoring purchases made under the Finance Policy.
- Overseeing purchase requests for electronic devices.

3. Classifications

Trust or school-owned and personal devices or ICT facilities include, but are not limited to, the following:

- Computers, laptops and software
- Monitors
- Keyboards
- Mouses
- Scanners
- Cameras
- Camcorders
- Other devices including furnishings and fittings used with them
- Mail systems (internal and external)
- Internet and intranet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Pagers
- Computers
- Photocopying, printing and reproduction equipment
- Recording and playback equipment
- Documents and publications (any type of format)

4. Acceptable use

This policy applies to any computer or other device connected to the trust and its schools' networks and computers.

The trust and its schools will monitor the use of all ICT facilities and electronic devices. Members of staff will only use trust or school-owned and approved personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching any trust or school-related task
- Any trust or school encouraged tuition or educational use
- Collating or processing information for trust or school business
- Effective communication, such as contacting the school office for assistance

Inappropriate use of trust or school-owned and personal devices could result in a breach of the trust's Data Protection Policy.

Inappropriate use of trust or school-owned and personal devices could result in a breach of legislation, including the UK GDPR and Data Protection Act 2018.

Any member of staff found to have breached the trust's Data Protection Policy or relevant legislation may face disciplinary action.

Staff will always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.

Trust or school-owned electronic devices will not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

Any illegal, inappropriate or harmful activity will be immediately reported to the principal.

Members of staff will not:

- Open email attachments from unknown sources.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- Upload or download large capacity files without permission from the ICT technician.
- Give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised school contact channels.
- Take an allocated school mobile phone out of the school premises, unless permitted by the principal.

All data will be processed appropriately in accordance with the trust's Data Protection Policy and Records Management Policy.

Members of staff will only use trust or school-owned electronic devices to take pictures or videos of people who have given their consent.

Trust or school-owned electronic devices will not be used to access personal social media accounts.

Personal electronic devices will not be used to communicate with pupils or parents, including via social media.

Staff will ensure they:

- Express neutral opinions when representing the trust or their school online.

- Avoid disclosing any confidential information or comments regarding the trust or their school, or any information that may affect their reputability.
- Have the necessary privacy settings applied to any social networking sites.

Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.

Copyrighted material will not be downloaded or distributed.

Trust or school-owned devices can be taken home for work purposes only, once authorised by the principal.

Trust or school equipment that is used outside the premises, e.g. laptops, will be returned to the school when the employee leaves employment, or if requested to do so by the principal.

While there is scope for staff to utilise trust or school equipment for personal reasons, this will not be done during working hours unless approved by the principal or in the case of a personal emergency.

Private business will not be mixed with official duties, e.g. work email addresses will be reserved strictly for work-based contacts only.

Use of a trust or school-owned phone for personal use will be permitted for necessary calls. A charge may be requested. Staff should seek appropriate authorisation to use a trust or school-owned phone for personal reasons on each occasion. The exception to authorisation is the use of the telephone system to make personal emergency calls; however, staff will notify the principal after the call.

Personal use of trust or school-owned equipment can be denied by the principal at any time. This will typically be because of improper use or over-use of school facilities for personal reasons. A charge may be made for using equipment if the values are significant.

Where permission has been given to use trust or school equipment for personal reasons, this use will take place during the employee’s own time, e.g. during lunchtime or after school. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours provided that disruption to the staff member’s work, and the work of others, is minimal.

Abuse of ICT facilities or devices could result in privileges being removed. Staff will be aware of acceptable ICT use, and misuse of the facilities, as defined in this policy, will be reported to the principal.

More details about acceptable use can be found in the Staff Acceptable Use of Technology Agreement.

Failure to adhere to this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

5. Emails and the internet

The trust and its schools' email systems and internet connections are available for communication and use on matters directly concerned with trust or school business.

Unprofessional messages will not be tolerated. All emails will be written in a professional tone and will be proof read by the staff member sending the email to ensure this prior to sending.

Abusive messages will not be tolerated – any instant of abuse may result in disciplinary action.

If any email contains confidential information, the user will ensure that the necessary steps are taken to protect confidentiality and personal data.

The trust and its schools will be liable for any defamatory information circulated either within the trust or to external contacts.

The trust and its schools' email systems and accounts will never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications. School or trust email addresses will not be shared without confirming that they will not be subjected to spam or sold on to marketing companies.

Emails that are sent or received will be retained within the school for a limited period dependent on the information contained. More information can be found in the Records Management Policy. The timeframe may be altered where an inbox becomes full.

All emails being sent to external recipients will contain the trust standard confidentiality notice. That notice will normally be configured as a signature by the ICT technician and will not be removed.

Personal email accounts will only be accessed via school computers outside of work hours and only if they have built-in anti-virus protection. Staff will ensure that access to personal emails never interferes with work duties.

Staff linking work email accounts to personal devices, subject to the principal's approval, will agree to submitting their devices for security checks on request.

The types of information sent through emails to a personal device will be limited to ensure the protection of personal data, e.g. pupils' details.

Contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the school, and the recipient. Staff will never commit the school to any obligations by email or the internet without ensuring that they have the authority to do so.

Purchases for school equipment will only be permitted to be made online with the permission of the principal and SBM/Bursar, and a receipt will be obtained in order to comply with monitoring and accountability. This is in addition to any purchasing arrangement followed according to the trust's Finance Policy.

Any suspicious emails will be forwarded to the CEO ceo@aspire.cheshire.sch.uk. No attachments on suspicious emails will be opened. All incidents will be responded to in accordance with the trust's policies and cyber security policy.

6. Portable equipment

All data on school-owned equipment will be regularly backed up in accordance with Cyber Security Policy.

Portable school-owned electronic devices will not be left unattended, and instead will be kept out of sight and securely locked in location when they are not in use.

Portable equipment will be transported in its protective case, if supplied.

Where the trust school provides mobile technologies, such as phones, laptops and personal digital assistants, for off-site visits and trips, staff will only use these devices.

The school will ensure that any school owned mobile phones have the necessary software and settings installed to meet data protection and safeguarding requirements.

Parents will not call school-owned mobile phones unless there are specific reasons for them to communicate directly with school staff such as managing their child's medical needs. In emergencies, parents will contact school's emergency contact number.

7. Personal devices

Staff members will use personal devices in line with the trust's Cyber Security Policy.

All personal devices that are used to access the trust and its schools' online portals, systems or email accounts, e.g. laptops or mobile phones, will be declared and approved by the principal before use and submitted, as requested, for the checks outlined in safety and security section of this policy.

Staff using personal devices must agree to and understand the requirement for security checks to take place and the possibility of their personal information being seen by the ICT support technician. They will be required to provide consent to their device being accessed – if consent is refused, they will not be permitted to use a personal device.

Approved devices will be secured with a password or biometric access control, e.g. fingerprint scanner. Passwords should comply with the trust's password policy.

Members of staff will not contact pupils or parents using their personal devices except in exceptional circumstances. In such circumstances, the phone number should be withheld.

Personal devices will only be used in exceptional circumstances for off-site educational purposes when mutually agreed with the principal.

Inappropriate messages will not be sent to any member of the trust community.

Permission will be sought from the owner of a device before any image or sound recordings are made on a personal device. Consent must also be obtained from staff, pupils and other visitors if photographs or recordings are to be taken.

Members of staff bringing personal devices into school will ensure that there is not any inappropriate or illegal content on their device.

During lesson times, unless required for the teaching activity being undertaken, personal devices will be kept in the school's agreed secure location.

8. Removable media

The trust and its schools will minimise the need to use of removable media with the intention of eliminating the use of removable media as soon as possible. This can be achieved through the use of secure cloud computing.

If removable media must be used, it will always be securely stored when not in use. Staff will be required to sign removable media devices in and out when they use them.

Personal and confidential information will not be stored on any removable media.

All removable media must be encrypted with appropriate security measures.

Removable media will be disposed of securely by the ICT technician.

9. Cloud-based storage

Data held in remote and cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018; therefore, members of staff will ensure that cloud-based data is kept confidential and no data is copied, removed or adapted.

10. Storing messages

E-mail is a communications tool, and e-mail applications are not designed for keeping e-mail as a record. E-mail that needs to be kept should be identified by content, for example:

- Does it form part of a pupil record?
- Is it part of a contract?
- Does it relate to an employee?

The retention for keeping these e-mails and messages should then correspond with the types of records found in the Records Management Policy. These e-mails and messages may need to be saved into an appropriate electronic filing system or printed out and placed on paper files. Similarly, information contained within these e-mails should be recorded in the appropriate place (e.g. the management information system (MIS) or behaviour management system). Once this is done, the original e-mail or message can be deleted.

E-mails in inboxes should be deleted after no more than six months, assuming they have been filed appropriately according to the nature of their content, as described above. .

Information and data on the trust and its schools' networks and computers will be kept in an organised manner and should be placed in a location of an appropriate security level.

If a member of staff is unsure about the correct message storage procedure, help will be sought from the principal, ICT technician or DPO.

Employees who feel that they have cause for complaint as a result of any communications on trust or school-owned devices will raise the matter initially with the principal, as appropriate. The complaint will then be raised through the grievance procedure in line with the Grievance Policy.

11. Unauthorised use

Staff will not be permitted, under any circumstances, to:

- Use the ICT facilities for commercial or financial gain without the explicit written authorisation from the principal.
- Physically damage ICT and communication facilities or trust and school-owned devices.
- Relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of the principal. Certain items are asset registered and security marked; their location is recorded by the SBM/Bursar for accountability. Once items are moved after authorisation, staff will be responsible for notifying the SBM/Bursar of the new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.
- Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. User account passwords will never be disclosed to or by anyone.
- Use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
  - Any material that is illegal
  - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
  - Online gambling
  - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
  - Any sexually explicit content, or adult or chat-line phone numbers
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Install hardware or software without the consent of the principal.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the trust and its schools' computers.
- Use or attempt to use the trust and its schools' ICT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
- Purchase any ICT facilities without the consent of the principal. This is in addition to any purchasing arrangements followed according to the Finance Policy.
- Use or attempt to use the trust and its schools' phone lines for internet or email access unless given authorisation by the principal. This will include using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, staff will not download or attempt to download any software of this nature.
- Use the internet for any auctioning activity or to purchase items unless given authority to do so by the principal. This is in addition to any purchasing arrangement followed according to the Finance Policy.

- Knowingly distribute or introduce a virus or harmful code onto the trust and its schools' networks or computers. Doing so may result in disciplinary action, including summary dismissal.
- Use the ICT facilities for personal use without the authorisation of the principal. This authorisation will be requested on each occasion of personal use.
- Copy, download or distribute any material from the internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If a staff member it is not clear that they have permission to do so, or if the permission cannot be obtained, they will not download the material.
- Use, or attempt to use, the communication facilities to call overseas without the authorisation of the principal.
- Obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school, its customers or suppliers.
- Interfere with someone else's use of the ICT facilities.
- Be wasteful of ICT resources, such as printer ink, toner and paper.
- Use the ICT facilities when it will interfere with their responsibilities to supervise pupils.
- Share any information or data pertaining to other staff or pupils at the school with unauthorised parties. Data will only be shared for relevant processing purposes.
- Operate equipment to record an image beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks without their knowledge or consent, whether exposed or covered by underwear – otherwise known as "upskirting".

Any unauthorised use of email or the internet may result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Procedure.

If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of trust or school-owned devices, they will report this immediately to the principal.

12. Loaning electronic devices

School equipment, including electronic devices, will be loaned to staff members in line with the school's policy.

13. Purchasing

Funding for electronic devices, predetermined by trust and the school's financial plan, will be available on request from the SBM/Bursar.

Requests for equipment or electronic devices will be made in accordance with the trust and its schools' agreed purchasing procedures.

Individual staff members will not be permitted to purchase equipment or devices, or process payments for such goods, on the trust or school's behalf unless permission has been sought from the principal.

The cost of any equipment or devices personally purchased by staff members will not be reimbursed by the school, unless otherwise specified by the principal.

In relation to devices for a specific project, project budget holders will provide evidence and a written statement requesting the necessary funds for the equipment required.

The SBM/Bursar will seek advice from the trust, ICT technician and other professionals when purchasing equipment.

All equipment and electronic devices will be sourced from a reputable supplier.

The SBM/Bursar will maintain a Fixed Asset Register which will be used to record and monitor the school's assets. All equipment and electronic devices purchased using school funds will be added to this register.

Old equipment or electronic device will be returned to the SBM, including any accessories which were originally included with the device. Any old devices will then be wiped clean by the ICT technician and disposed of securely.

14. Safety and security

The trust and its schools' networks will be secured using relevant security devices and software in line with the Cyber Security Policy in order to prevent unauthorised access to the systems.

Filtering of websites, as detailed in the Cyber Security Policy, will ensure that access to websites with known malware are blocked immediately and reported to the ICT technician.

Approved anti-virus software and malware protection will be used on all approved devices and will be updated as required.

The trust and its schools will use mail security technology to detect and block any malware transmitted via email – this will be reviewed regularly as detailed in the Cyber Security Policy

Members of staff will ensure that all trust and school-owned electronic devices are made available on request for anti-virus updates, malware protection updates and software installations, patches or upgrades. Where devices are set up to update automatically, members of staff will ensure the upgrade is successfully installed. Support will be sought from the ICT technician by members of staff if they require it to keep the devices they use safe and secure.

Approved personal devices will also be submitted on request, to the ICT technician, so that appropriate security and software updates can be installed to prevent any loss of data. Consent for such access will be obtained before the approval of a device – if consent if refused, the trust and its schools reserve the right to decline a request to use a personal device.

Programmes and software will not be installed on trust and school-owned electronic devices without permission from the ICT technician.

Staff will not be permitted to remove any software from a trust or school-owned electronic device without permission from the ICT technician.

Members of staff who install or remove software from a trust or school-owned electronic device without seeking authorisation from the ICT technician, may be subject to disciplinary measures.

All devices will be secured by a password or biometric access control.

Passwords will adhere to the trust's password policy, be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.

Multifactor authentication will be used whenever possible.

Devices will be configured so that they are automatically locked after being left idle for a set time. This will be no more than 10 minutes for mobile or other portable devices and 15 minutes for desktop computers or laptops.

All devices must be encrypted.

Further security arrangements are outlined in the Cyber Security Policy.

15. Loss, theft and damage

For the purpose of this policy, **"damage"** is defined as any fault in a trust or school-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the ICT technician
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

Incidents and the circumstances of damage or loss will be considered by the principal on an individual basis.

The principal will consider whether the loss, theft or damage of trust/school owned electronic devices is covered by the school's Risk Protection Arrangement (RPA) for academy trusts membership.

If it is decided that a member of staff is liable for the damage or loss, they may be required to pay towards the repair or replacement cost.

The ICT technician will be informed if a trust or school-owned electronic device has a technical fault.

If a school-owned device is lost or stolen, or is suspected of having been lost or stolen, the principal and DPO will be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to the trust or school, its staff and its pupils, and that the loss is reported to the relevant agencies.

The trust and its schools will not be responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

16. Implementation

Staff will report any breach of this policy to the principal.

Regular monitoring and recording of email messages may be carried out on a random basis. Hard copies of email messages can be used as evidence in disciplinary proceedings.

Use of the telephone system will be logged and monitored.

Use of the school internet connection will be recorded and monitored.

The SBM will conduct random checks of asset registered and security marked items.

The ICT technician may, at the request of the principal, remotely view or interact with any of the computers on the trust and its schools' networks. This may be used randomly to implement this policy and to assist in any difficulties.

Each school's network has anti-virus software installed with a centralised administration package; any virus found will be logged to this package.

Schools' database systems are computerised. Unless given authorised access rights by the principal, members of staff will not access these systems. Failure to adhere to this requirement may result in disciplinary action.

All users of the database system will be issued with a unique individual password. Staff will not, under any circumstances, disclose this password to any other person.

Attempting to access the database using another employee's user account and/or password without prior authorisation, other than in an exceptional circumstance, may result in disciplinary action, including summary dismissal.

User accounts will be accessible by the principal and any other authorised administrators with support from the ICT technician.

Users will ensure that critical information is not stored solely within the school's computer system. The trust and its schools' data will be backed up regularly as detailed in the Cyber Security Policy. Hard copies of essential, critical information may be kept securely.

Users will be required to familiarise themselves with the requirements of the UK GDPR and Data Protection Act 2018, and to ensure that they operate in accordance with the requirements of the regulations and the Data Protection Policy.

Any breach of this policy may result in disciplinary action, which may lead to dismissal.

A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the school.

17. Monitoring and review

This policy will be reviewed in accordance with the trust's policy review schedule.

Any changes or amendments to this policy will be communicated to all staff members.