The Auriga Academy Trust

# IT Security and Acceptable Usage Policy

## CONTENTS:

## 1 Introduction

The Trust's / school's IT (Information Technology) infrastructure and digital resources are essential to the effective delivery of education and other activities, but they also present risks to data protection, online safety and safeguarding. The Trust is committed to using IT facilities in a way that meets legal requirements and upholds confidentiality and peoples' privacy rights.

This policy supports business continuity, data protection and cyber security, and explains how the Trust and its constituent schools use technology in line with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), the Departments for Educational Digital and Technology standards in schools and colleges and other relevant legislation.

## 2 Scope and Responsibilities

This policy applies to:

- The use of school-provided (or provided for the school's use) IT hardware, software, devices, digital content, networks and communications.
- Non-school owned devices which are used for accessing school Internet or information systems or used in a way which impacts on the school or school community.
- All those who access school systems including pupils, staff, visitors, governors. These are all referred to as "Users" throughout this policy.

All Users are responsible for reading, understanding and complying with this procedure if they have access to IT. Whilst this policy applies to all Users, the Trust / school understands that pupils will need additional support to understand how to use IT systems safely and securely.

## 3 IT Acceptable Use Standards

All Users must:

1. Protect Trust / school IT resources by careful and considerate use of equipment and networks, reporting faults and minimising the risk of introducing computer viruses or similar to the system.
2. Protect individuals from harmful or inappropriate material accessible via the Internet or electronic media.
3. Protect the confidentiality of individuals and of school matters and safeguard users by complying with relevant legislation, including:
    - Data Protection Act 2018 and General Data Protection Regulation
    - Privacy and Electronic Communications Regulations
    - Copyright, Designs and Patent Act 1988
    - Computer Misuse Act 1990
    - Counterterrorism and Security Act 2015 (encompassing the "Prevent Duty")
    - The Regulation of Investigatory Powers Act (RIPA) 2000
    - Waste Electrical and Electronic Equipment Regulations 2006, the Environmental Protection Act 1990, the Waste Management Regulations 2006.
    - The Department for Education Cyber security standards for schools and colleges
    - Broadband internet standards for schools and colleges
    - Switch standards for schools and colleges
    - Network cabling standards for schools and colleges
    - Wireless network standards for schools and colleges

Users should understand and adhere to their signed **Acceptable Use Agreement (Appendix 1)**.

## 4 Roles and Responsibilities

Everyone who works for The Auriga Academy Trust has a responsibility to ensure that data is collected, accessed, stored and handled appropriately and lawfully. Every user must ensure that they adhere to this policy in order to meet the legal obligations of the Trust / school and their individual obligations.

The Trust's Board of Trustees, whilst ultimately responsible for ensuring the Trust meets its legal obligations, is assisted directly by the senior leadership team.

Breaches of this policy should be reported to Trust / school senior leaders in the first instance and where there is a data breach must be reported on GDPRiS.

## 5 Principles of Use

For the purpose of this policy, the use of the internet will include associated internet-enabled technologies such as, cloud based systems (such as O365, MIS (ARBOR) , Safeguarding (POMS), Remote learning platforms), emails, video calls, video messaging, instant messaging, webinar applications or conferencing applications.

- Internet and email use is integral to the effective delivery of services provided by the Trust / school. Nothing in this policy should be read as restricting the proper use of email, Internet or associated technologies for Trust / school purposes.
- Limited personal use of a school's Internet is permitted subject to these principles and guidance notes.
- Personal use of the Internet is only permitted in an employee's own time (e.g. before or after work and during lunchtime) and limited to browser-based activities. Any personal use must not, in any way, distract staff from the effective performance of their duties. Improper or inappropriate personal use of a school's email, Internet and associated systems may result in disciplinary action.
- Users are not allowed use of the Trust / school's email system for personal communication.
- If an employee feels they may have accidentally breached this policy, they should contact their line manager immediately, or, in their absence, a more senior manager who will address the situation. See Unacceptable Use – Section 5.
- The Trust / school reserves the right to maintain and review usage logs of the school IT services including the internet and associated internet-enabled technologies including emails, video calls, video messaging, instant messaging, webinar applications or conferencing applications and email use. Auditing and monitoring of the use of Trust / school IT services may form part of disciplinary procedures.
- The Trust / school has in place a process to block categories of internet sites and individual sites if it is deemed appropriate. Users must not attempt to bypass security measures or processes.
- Any personal information sent via email, the Internet and associated internet-enabled services is covered by Data Protection legislation. All staff are required to handle personal information in accordance with the Data Protection Act 2018 and the UK GDPR.
- Emails, including conversations recorded using facilities such as video calls, instant messaging or conferencing applications, are covered by the Freedom of Information (FOI) Act and may be disclosed as part of an FOI request for information, or as part of any legal proceedings. Staff are reminded to always exercise the same caution on email content, video calls, instant messaging or conferencing applications as in more formal correspondence.
- Whilst Trust / school security provides additional protection and real-time scanning, our security measures cannot guarantee that external communications do not contain malicious content or links. All staff with access to the IT network must take basic cyber security training annually in line with DfE Cyber Security Standards.
- Consent from all parties must be obtained before recording conversations when using facilities such as video calls, instant messaging or conferencing applications.
- The Trust / school reserves the right to withdraw Internet access or email use or any access to the Trust / school's computer or communications network, if a user is found to be in breach of this policy.
- Desktop and document sharing capabilities via facilities such as video calls or conferencing applications, must only be used with colleagues of the Trust / school for collaboration purposes. If changes are to be made to these documents during a desktop sharing session, the 'sharer' of the document has the responsibility of ensuring that the documentation is used correctly and saved appropriately.

## 6 Email

### 6.1 Personal Use

Personal use of school email is not permitted. However, communication with a Trade Union is not considered personal use. It is inappropriate to use a school address for personal use as it may give the impression that any business is on behalf of the Trust / school.

If a genuine emergency arises users should inform their line manager at the earliest opportunity that they have responded to the email and managers will make a note of it. Users should inform the sender that personal use of the Trust's / school's email system is not permitted and provide an alternative email address or an alternate method of communication.

### 6.2 Email Usage

Users are not permitted to send and receive Trust / school related information from personal email accounts. Users must only use Trust / school provided email systems. However, staff are permitted to forward emails to their Trade Union representative via their personal email account, for the purposes of seeking advice.

If users receive an email that is inappropriate or abusive, they must report it to their line manager immediately, who will take the appropriate action. If the sender is known to the user, they should inform the sender to cease sending the material.

Users must not use anonymous mailing services to conceal their identity or falsify (spoof) emails to make them appear as if they have been sent from someone else.

All employees are required to maintain the good reputation of the Trust and its constituent school when using Internet and email. Users must not use the email system in any way that is unprofessional inappropriate or harmful.

Use of email and the Internet which brings the Trust / school into disrepute may result in disciplinary action.

### 6.3 Email Disclaimer

A disclaimer is automatically attached to all emails sent from the Trust / school system informing the recipient that the email is intended solely for them, is confidential, may be legally privileged and may contain personal views that are not those of the Trust / school.

Recommended wording is as follows: This email and its attachments may be confidential and are intended solely for the use of the intended recipient. If you are not the intended recipient of this email and its attachments you must take no action based upon them, n or must you copy or show them to anyone. Please contact the sender if you believe you have received this email in error. Any views or opinions expressed are solely those of the author and do not necessarily represent those of The Auriga Academy Trust [insert name of school], unless otherwise specifically stated.

### 6.4 Access to email

When an employee is absent, the employee's line manager can authorise access to a Trust / school email account to obtain messages that are work-related. The manager will inform the employee of this access on the employee's return.

The content of all emails may be viewed by the Trust / school in certain circumstances, for example, in connection with disciplinary investigations or audit reviews.

### 6.5 Email Security

Emails containing sensitive personal data, or otherwise sensitive information, must be sent securely. Any personal data sent externally by email must be sent with encryption enabled or via a password protected file with the password sent via alternative means e.g. telephone.

All senders must ensure the appropriate secure email method is chosen according to the circumstances of the destination of the email.

Senders of any controlled/restricted email must be extremely vigilant about verifying the recipient's email address to ensure sensitive data is not sent to the wrong individual/s, leading to a data breach.

Personal data sent to the incorrect recipient should be reported in line with Trust's / school's Data Breach Procedure.

When emailing multiple recipients, the 'TO' box should be addressed to an address within the organisation (eg info@school.sch.uk) and the BCC option (blind copy) chosen to add multiple email addresses so addresses are not disclosed.

### 6.6 Email Retention

It is recommended that emails are routinely deleted if older than 6 months. Any emails that need to kept beyond this period should be saved to appropriate file storage. For further information, please refer to the **Trust's Document Retention Schedule**.

All electronic communications, whilst they are held by the Trust / school, are potentially disclosable under data protection legislation and anything within an email could be released in response to a Subject Access Request.

### 6.7 Out of Office

Email accounts should return an Out of Office message during school holidays. This will indicate whether or not emails will be monitored and when the Trust / school reopens. Similarly, during periods of extended staff absence an Out of Office message should refer senders to an alternative or general school email address. If an employee has failed to do this, the employee's line manager can authorise access to a Trust / school email account to set this up.

## 7 Instant Messaging (IM)

Instant Messaging is a form of real time communication between two or more people based on typed text. The text is conveyed via devices connected over the Internet or an internal network/intranet. Currently the Trust does not provide internet messaging (IM) services as email is the preferred method of communication.

## 8 Recording calls / meetings / online lessons / staff training

Recording calls, meetings, online lessons, etc will generate personal data including pupil images, names, contributions, and contact details and will be protected, processed and retained in the same way as all personal data, in line with the Trust's **Data Protection Policies** and **Privacy Notices** and in accordance with other policies including **Off Site Working** and **Bring Your Own Device** policies, as well as the Trust's **Data Retention Schedule**. The Trust / school recognises that recording staff whilst at work may be considered to be privacy intrusive and therefore careful safeguards will be put in place should recording be deemed necessary. In particular, the Trust and its schools must ensure that the Data Protection principles as set out in the **Data Protection Policy** are adhered to.

The Trust / school will never record calls, meetings, online lessons or staff training in a covert manner. Recordings in these circumstances will be carried out in line with Trust HR policies.

### 8.1 Recording telephone calls

The Trust / schools do not record incoming and outgoing telephone calls.

### 8.2 Recording meetings

The Trust / school may record meetings. The purpose of this is to ensure minutes and notes taken are an accurate record. Attendees will be informed if the meeting is to be recorded. Recordings will be securely destroyed as soon as the minutes have been approved. Recordings will be available to attendees until minutes are approved and the recording destroyed.

### 8.3 Recording online lessons

The Trust schools do not record online lessons.

### 8.4 Recording staff training

The Trust / school may record staff training. The purpose of this is to ensure the training is available to staff who were unable to attend live. Attendees will be informed if the training is to be recorded. Protocols regarding cameras, chats and contacts will be outlined at the start of each session. Additional information about the lawful basis, processors, use and retention period can be found in the Trust **Privacy Notices** and **Data Retention Schedule**.

## 9 Internet Use

### 9.1 Personal Use

Personal use of the Internet is not allowed during working hours. Employees can use the Internet, for browser-based activities only, before they start work, during their lunchtime, or after work. Staff must not, in any way, distract others from their work.

Employees must not use the Trust / school's Internet or email systems for trading or personal business purposes.

Employees are advised not to conduct online payments. This is due to the information being stored locally on a computer, which potentially could be compromised, putting the user at financial risk. If an employee uses the Internet to buy goods or services, the Trust / School will not accept liability for default of payment or for security of any personal information provided. Goods must not be delivered to a Trust / school address.

All Internet browsing sessions should be terminated as soon as they are concluded.

### 9.2 Filtering Content

Many Internet sites that contain unacceptable content are blocked automatically by the Trust / school's systems. However, it is not possible to block all "unacceptable" sites electronically in all circumstances.

Attempting to bypass or disabling filtering, proxy or security settings is strictly forbidden without written authorisation from the CEO / Headteacher.

Where it is necessary to disable services temporarily, the business need for the action will be documented and the risks assessed. Approval from the CEO (Trust central staff) / Headteacher (school staff) must be sought and services must be re-enabled / any open ports closed, as soon as possible.

Filtering requirements form part of the Prevent Duty, as enacted in the Counter-Terrorism and Security Act 2015.

### 9.3 Downloading Material

Users must not download-video, music files, games, software files and other computer programs. These types of files consume large quantities of storage space on the system (and can slow it down considerably) and may violate copyright laws.

Streaming media, such as radio or TV programmes, for non-work-related purposes is not permitted.

If you are in doubt about software use or installation, seek guidance from the Headteacher and/or Finance Director who will liaise with the Trust's Data Protection Officer.

### 9.4 Accidental Access to Inappropriate Material

An employee may receive an email or mistakenly visit an Internet site that contains unacceptable material. If this occurs, they must inform senior leadership immediately.

The senior leadership will ask you for details of the incident including how the event occurred. This information may be required later for management and audit purposes.

### 9.5 Copyright

Downloading and copying data and software or sending the work of others to third parties without permission can infringe copyright. Most sites contain a copyright notice detailing how material may be used. Copyright should be checked and appropriate permissions sought. Simply cutting and pasting material from one source to another may be in violation of copyright laws. All sources used for research purposes should be referenced appropriately and credited. In the case of subscription services the appropriate licenses must be obtained. If an employee is in any doubt about downloading and using material for official purposes, legal advice should be sought to ensure compliance with the Copyright, Designs and Patents Act 1988. Support can also be requested from The Trust Finance Director.

The Trust retains the copyright to all materials produced by an employee in the course of their duties, including any original ICT based material produced.

### 9.6 Unacceptable Use

Employees must not deliberately view, copy, create, download, save, print or distribute any material that:

- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material the possession of which would constitute a criminal offence
- promotes any form of criminal activity
- contains unwelcome propositions
- involves gambling, multi-player games or soliciting for personal gain or profit

- contains images, cartoons or jokes that may cause offence
- appears to be a chain letter
- brings the School into disrepute or exposes it to legal action

This list is not exhaustive and the Trust / school may define other areas of unacceptable use. Unacceptable use may be reported to the police if likely to constitute a breach of the Computer Misuse Act 1990.

## 10 Monitoring

The Trust / school is able to produce monitoring information, which may include email usage statistics, frequent email contacts, file sizes and may lead to making further enquiries.

The Trust / school is also able to record the details of all Internet traffic to protect the Trust / school and its employees from security breaches, including hacking, and to ensure that "unacceptable" sites are not being visited.

Any potential infringement will be referred to Senior Leadership as part of routine reviews.

The Trust / school may read and inspect individual emails and attachments for specific business purposes or during disciplinary investigations including:

- Establishing the content of transactions,
- Ensuring employees are complying both with the law and with the Trust's email policy, and
- Checking emails when employees are on leave, absent or for other supervisory purposes.

The Trust / school's email system records details of all emails sent and received. The system filters the use of certain prohibited words and may limit file sizes. Monitoring logs may include:

- The network identifier (username) of the user
- The address of the Internet site being accessed
- Where access was attempted and blocked by the system
- The web page visited and its content
- The name of any file accessed and/or downloaded
- The identity of the computer on the network and the date and time

Any excessive or inappropriate use may result in disciplinary action being taken.

Interception of communications must be carried out in compliance with the Investigatory Powers Act 2016.

## 11 Passwords and Multi-factor Authentication

Passwords are an essential element of network security. The below guidelines apply to all users of Trust systems. 'Users' is defined as employees, agency staff, Trustees and Governors, contractors, volunteers and vendors who

- have or are responsible for any network account or resources (or any form of access that supports or requires a password) on any system that resides at any Trust site.
- have access to the Trust's data network.
- store any personal, sensitive or confidential Trust information.

### 11.1 Managing Passwords

The continual reliance on IT systems, requires that effective password controls are in place to ensure that the integrity of all system/access logon accounts used across the Trust are maintained. The following procedures and practices must be followed to ensure the security and integrity of these accounts.

- All users must ensure that their password is not divulged or shared with anyone else.
- All users must not write down and store passwords.
- Passwords must not be inserted into email messages or other forms of electronic communication with the exception of some systems/processes which may require automatically generated temporary passwords to be sent. Temporary passwords must be changed as soon as possible.
- All ICT devices which may require local logon privileges for configuration and maintenance i.e. Printers, network switches, routers etc. must all have the built-in default admin (or equivalent) account password changed in line with the guidelines of this policy wherever possible.
- Consideration should be given in the use of Multi-Factor Authentication (MFA) wherever possible or appropriate.

11.2 Choosing a Password

When choosing a password, the NCSC recommend creating a password from 3 randomly selected words. Users should choose words that are memorable but should avoid those which might be easy to guess, such as 'Onetwothree123' or are closely related to the user, such as the names of family members or pets. For example 'blueberry train crash' can create a passwords that is long enough and strong enough. Including the recommendation to include a symbol, and upper and lower case letters, a good password example would be blueberry?Traincrash7. Ultimately, the choice of password is up to the user.

11.3 Setting a password for logging on to a pc/laptop

A users first logon to a pc or laptop is the security boundary for the majority of systems in use and safeguards against unauthorised access to sensitive data. Whether a school is Microsoft Office or Google based the following password configuration rules apply.

- Passwords must be 12 or more characters.
- Passwords must contain at least 1 Uppercase, 1 lowercase and 1 numerical digit. It is strongly recommended that a symbol is also used within the password.
- Account will be locked for 30 minutes after 6 wrong password attempts.
- No re-use of last 24 passwords.

11.4 Multifactor authentication

Multi-factor authentication (MFA) is a multi-step account login process that requires users to enter more information than just a password. For example, along with the password, users might be asked to enter a code sent to their phone. The NCSC Cyber Essentials requires that authentication to cloud services must always use MFA, this includes Microsoft Office and Google services. When users log into any Trust / school android device for the first time MFA will be required using an authentication app. However, should a user then log in from a different devise, MFA will be required again using the app.

11.5 Virtual Private Network (VPN) Users (CISCO - AnyConnect) – Trust Staff

Due to the nature of the VPN connection, users are required to create a strong 12 character password and download an authenticator app. VPN users are required to undertake MFA every time they log in.

11.6 Password Protection Standards

All users are required to adhere to the following list of "Don'ts":

- Don't use the same password you use for Trust / School accounts as for other non-Trust / non-school access (e.g., personal ISP account, personal banking, online shopping etc.).
- Don't share Trust / school passwords with anyone including your line manager. All passwords are to be treated as sensitive, confidential information. If someone demands a password, refer them to this document and request that they discuss the matter with Senior Leadership.
- Don't reveal a password over the phone to ANYONE - unless relaying information on temporary passwords which are changed immediately.
- Don't write passwords down and store them anywhere in your class / office.
- Don't reveal a password in an email message - unless relaying information on temporary passwords which are changed immediately.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on holiday.
- Don't use the "Remember Password" feature of applications (e.g., Internet Explorer, SAP etc...).
- Don't store passwords in a file on ANY computer system (including mobile devices or similar) without encryption.

If an account or password is suspected to have been compromised, report the incident as soon as possible to the IT Support AND log this as a potential data breach on GDPRiS. Immediately change any/all passwords which may have been compromised.

## 12 Loaned IT Equipment

The Trust / school provides access to ICT to enable employees to undertake their duties as specified by their job description. Access to ICT through the Trust / school is not intended for personal use, please see paragraph 6 for further information. On this basis, the CEO / Headteacher, or another designated senior person, has authority to obtain access to an employee's data and documents, including emails.

Employee's wishing to use Trust / school ICT equipment (e.g. laptop / chrome book) at home must seek permission from their line manager and sign the relevant documentation accepting responsibility for loss or damage. Please see Appendix 2: School Equipment Agreement.

Devices issued to staff remain the property of the Trust / school and are provided to users on a loaned basis. The device must not be used by anyone other than the authorised user to whom it has been allocated.

Any device property identification must not be altered or removed for any reason.

Users who borrow equipment from the school must sign for it and bear the responsibility for its care. Please see Appendix 2: School Equipment Agreement.

All reasonable care should be taken to prevent loss, damage, theft or unauthorised use of IT equipment. Devices should never be left in a vehicle or other unsecured, vulnerable situation. See the **Offsite Working Policy** for more guidance.

Any loss or damage to equipment on loan should be immediately reported to the CEO (Trust central staff) / Headteacher (school staff) in the first instance and any theft or criminal damage should be reported to the Police AND logged on GDPRiS as a potential data breach.

Where there is evidence that the equipment has not been used in accordance with policy, a charge may be made for the replacement or repair of any school equipment whilst on loan.

## 13 Bring Your Own Device (BYOD)

Employees are permitted to use their own ICT equipment during breaks. However, personal ICT equipment can only be used in a place not accessible to students.

To prevent data loss and ensure consistent application of School policies, no personally owned equipment should be attached to a school's network without the permission of the CEO (Trust central staff) / Headteacher (school staff).

Please refer to the separate Trust **Bring Your Own Device (BYOD) Policy.**

## 14 Software, Updates and Patching

School devices have a predetermined list of software installed on the hard drive.

Users should use software in accordance with applicable licence agreements. It is a criminal offence to copy software or any supporting documentation protected by copyright. Employees must not transfer any software licensed to the school or data owned or licensed by the school without authorisation from the CEO (Trust central staff) / Headteacher (school staff) or the designated ICT person.

Software can only be downloaded with permission from the CEO (Trust central staff) / Headteacher (school staff) and the designated authorised ICT person. Downloaded software becomes the Trust's / school's property and must be used only under the terms of its license. Employees must arrange to license and register such software, where required. Software downloaded without permission must be deleted.

The use, or possession of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited by the Trust / school.

No addition or deletion of any software or hardware (except peripherals) is permitted without the express permission of the CEO (Trust central staff) / Headteacher (school staff). This includes the setting up of web-based accounts.

Software and web-based accounts that use personal data may be subject to a Data Protection Impact Assessment and must not be installed or set up until this has been carried out by the Finance Director.

To ensure that security patches and virus definitions are up to date staff must connect devices to the Trust / school network on a regular basis. Updates must be allowed to run and should not be interrupted.

Staff should make careful, considerate use of the school's IT resources, report faults and work in a way that minimises the risk of introducing computer viruses into the system.

## 15 Network Access and Data Security

### 15.1 Users' Authorisation

Those accessing information systems, data or services will be authorised to do so by an appropriate authority, usually their line manager.

Changes to access must be requested and authorised. Users who believe they have access to systems they no longer need, must report this to their line manager or Headteacher.

Users must only access information held on the Trust's / school's computer systems if authorised to do so and the information is needed to carry out their work.

Line managers will only request the minimum access required for the user to carry out their work.

A record of user access to systems (**Data Access Register**) will be maintained and periodically reviewed by Trust HR and updated for starters and leavers.

### 15.2 Starters, Movers and Leavers (Account Creation, Approval and Removal process)

Line managers, with the support of admin and HR, must ensure that access to IT Systems is only available to employees during their period of employment and withdrawn as soon as employment is terminated.

The same principles apply to pupils joining and leaving the school.

System access arrangements for new starters are controlled by Trust HR. Trust HR will liaise with the relevant IT support and school administration to ensure the necessary access arrangements are granted.

When a contract of employment at the Trust ends, the member of staff must return all equipment, including peripherals, to the Trust / school in full working condition.

It is the responsibility of the user to backup any data or documents they may require, prior to returning the device. Any data pertaining directly to the school or members of the school community **must not** be retained.

Retaining any personal data without the authorisation of the Trust / school is an offence under the Data Protection Act 2018.

The user account and all personal work stored on the laptop will be securely deleted upon return.

### 15.3 External Support Access

Staff providing temporary guest logins for external support services providers must ensure that system access does not extend beyond the requirements for the provision of services.

Those requesting/providing temporary access must also ensure that system access is withdrawn as soon as the affiliate's relationship with the school ceases.

### 15.4 Confidentiality

Under no circumstances should personal or other confidential information held on the school network or IT equipment be disclosed to unauthorised persons. If a staff member, agency member of staff, Governor, or Trustee accidentally has access to information which they are not entitled to view, they should report this immediately to the CEO (Trust central staff) / Headteacher (school staff) as a data breach. It must also be logged on GDPRiS.

Staff must ensure that confidential or sensitive data is not accessible to unauthorised persons by logging off or locking the computer when it is left unattended.

In classrooms, screens must be set to **extend** to the Interactive whiteboard rather than **duplicate** and when using screen sharing facilities, users should fully close or minimise screens with any sensitive data / emails.

### 15.5 Security of Portable Devices

The Trust / school does not allow the use of USBs / removable storage devices.

Sensitive or confidential information should be accessed via the network and should not be permanently stored on portable devices e.g. memory sticks / laptops / tablets.

Where the use of a memory stick to transfer or store data temporarily is unavoidable, this must be done using an encrypted memory stick provided by the Trust / school.

All Trust / school devices used to store personal information will be fully encrypted.

### 15.6 Physical Security

Building access and physical controls protect areas where sensitive or confidential information is processed. Server access and access to network equipment, telecoms and network access points is restricted to those staff with authorisation.

### 15.7 Administrative Access

Administrative accounts and credentials must use strong authentication / complex passwords. Current guidance on the authentication and security measures that should be put into place for network devices, filtering and monitoring services and administrative accounts can be found in the DfE Cyber Security Standards.

Administrative accounts must not be used for general activities, especially those of high-risk, such as browsing the internet or emailing.

Administrative access is only provided to designated staff and a review of administrators for each system will be carried out termly by Trust HR, including administrative accounts that have not been used for a prolonged period of time, in line with the DfE Cyber Security Standards.

## 16 Disposal of Computing Resources

Computing resources will be disposed of in line with WEEE regulations, The Hazardous Waste Act, The Environmental Protection Act 1990, The Environment Act 1995 and The Data Protection Act 2018

1. All equipment which contains sensitive files will have their hard disk drives wiped and all sensitive or confidential data and licensed software will be irretrievably deleted during the disposal process.
2. Damaged devices containing sensitive or confidential data will undergo assessment to determine if the device should be destroyed, repaired or discarded.
3. If a third party contractor is used, suppliers will be suitably accredited and disposal certification will be obtained.
4. Finally, the Trust / school's asset inventory will be updated.

## 17 Backup Procedures

If software/hardware problems arise, a device may need to be restored to its original settings. Work files may be lost during the restore process, therefore it is the responsibility of all Users to ensure that files are saved to network drives or cloud-based networks.

Removable storage, such as encrypted USB's are not backed up by the routine backup process and users take responsibility for carrying out a manual backup process.

The Trust / school ensures that systematic backup of data is completed on a regular basis so that recovery of essential data can be managed in the event of loss of data files or system failure.

All servers maintained by Trust schools have 3 backup copies on at least 2 separate devices, with one of these being off-site. Backup copies are securely stored against theft, corruption or physical damage, so that in the event of a major incident a backup copy is available.

For Office based schools, and the Trust, additional O365 back up is in place for specified user accounts.

For Google based schools Senior Leadership and Teacher Google accounts are backed up.

## 18 Disaster Recovery Procedures

In the case of a disaster staff should refer to **the Business Continuity and Disaster Recovery Plan and/or Cyber Response Plan**. The plan includes the following as per the DfE Cyber Security Standards:

- staff responsibilities
- out of hours contacts and procedures
- internal and external reporting and communications plans
- priorities for service restoration
- the minimum operational IT requirements
- where you can find additional help and resources

Hard copies of key information should be kept in case of total system failure, and the plans should be regularly tested and reviewed.

## 19 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Trust / school assets, or an event which is in breach of the Trust's / school's security procedures and policies.

All Trust employees, supply staff, Governors, Trustees, contractors, and volunteers have a responsibility to report security incidents and breaches of this policy as quickly as possible to the CEO (Trust central staff) / Headteacher (school staff). This obligation also extends to any external organisation contracted to support or access the Information Systems of the School.

The Trust / school will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place.

Suspected misuse of a school's computer systems by a member of staff will be considered by the CEO and Headteacher, to determine whether further action is appropriate. In the case of an individual then the matter may be dealt with under the disciplinary process.

## Appendix 1: Statement of Acceptance of the Terms and Conditions of the AAT IT Security & Acceptable Usage Policy

I agree to follow the rules set out in the ICT Usage Policy.

I will use the Trust's / school's ICT network in a responsible way and observe all the restrictions explained in the Policy. If I am in any doubt I will consult _____ *[insert name of CEO (Trust central staff) / Headteacher (school staff)]*.

I agree to report any misuse of the school's ICT network to _____ *[insert name of CEO (Trust central staff) / Headteacher (school staff)]*.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to _____ *[insert name of CEO (Trust central staff) / Headteacher (school staff)]*.

I understand that any breaches of the Policy may result in loss of access to the ICT facilities and will be subject to disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Name of Employee: _

Signature of Employee: _

Date: _

## Appendix 2: Trust / School Equipment Agreement

**EQUIPMENT ASSIGNED:**

Item: (e.g. laptop, iPad, Chromebook):

---

Serial Number:

---

I assume responsibility for the equipment assigned to me and will adhere to the following -

The equipment is:

- used appropriately and only for Trust / school use
- NOT used to access any information that would put pupils in danger or the Trust / school into disrepute
- NOT used to access any social medial platforms, e.g. Instagram and face book
- NOT lent to anyone outside of school
- stored securely and I recognise I am responsible for the equipment whilst travelling. I accept personal liability for this equipment and acknowledge that I will bear the cost of the equipment in the event of damage or loss due to theft or otherwise.
- I will report any defects, faults, accidents, damage or loss immediately to school including reporting to the police if appropriate.

**Receiving:**

Signature: _____Date: _____

**Issuing Staff:**

Signature: _____Date: _____

**Returned by:**

Signature: _____Date: _____

**Received by:**

Signature: _____Date: _____

| The AURIGA Academy Trust Document Control System | |
|---|---|
| **NAME OF DOCUMENT** | AAT IT Security and Acceptable Usage Policy |
| **STATUS** | **APPROVED** |
| **DATE APPROVED** | 01.09.2024 |
| **APPROVER** | CEO |
| **OWNER** | Finance Director |
| **GOVERNANCE REVIEWER** | TBD |
| **ANTICIPATED REVIEW DATE** | 01.09.2028 |
| **LOCATION** | Word – AAT Team Share - Policies<br>PDF – Governors and Trustees – Board – Board Policies and Procedures |