CMAT ACCEPTABLE USE POLICY FOR ICT

A thriving family of schools who work together to celebrate differences, and support each other in pursuit of excellence.

DOCUMENT CONTROL

This document has been approved for operation within:	All Chancery schools.		
Responsible Officer:	DPO		
Approved by:	Board of Trustees		
Approval date:	09.07.2025		
Date effective from:	Sept 2025	**Date of next review:**	Summer 2028
Review period:	3 Year	**Version:**	2

Summary of changes within this version

Linked policies and related guidance have been updated.

Statements added relating to:

- Use of personal devices at home used for work purposes
- Use of mobile phones and smart watches
- Use of personal devices for photography
- Reporting of misuse

Other minor changes throughout.

Acceptable Use Policy for ICT

Information Technology (IT) is an increasingly integral part of school activities and is essential in the delivery of most services. Most school employees will use the school's Information Communication Technology (ICT) in the course of their duties.

This policy is designed to enable the School to:

- get the best return possible for the investment it has made in technology
- gain maximum benefit from email and the internet
- comply with the law
- minimise legal and other risks associated with the use of technology
- ensure effective running of the school's business
- minimise the risk of disruption caused by computer viruses and inappropriate use of IT; and
- provide clear information to employees and to increase ICT skills of our employees.

This document sets out the school's policy on using its computers and networks, including all devices such as telephones, mobile phones; printers, scanners and anything of an electronic nature otherwise referred to as information technology etc. This equipment is, for clarity of understanding, referred to throughout this policy as the Systems.

This policy applies to all school employees who use the Systems. It also applies to other people using the Systems such as agency workers, contractors, staff and volunteers.

This policy should be read in conjunction with the following:

- CMAT Data Protection policy
- CMAT Cyber Security Policy (due Autumn 2025)
- CMAT Social Media Policy
- CMAT Staff Code of Conduct
- School Online Safety Policies

It is based on guidance for schools from the National Cyber Security Centre and has regard to the DfE's digital and technology standards which are designed to provide a safe and secure environment for the use of technology.

Employees should be aware that the school Systems including the internal and external e-mail system may be monitored from time to time to ensure that the system is not being abused, to ensure that this policy is being complied with and for any other lawful purpose.

If you are unsure about how a rule or requirement applies then discuss with the Headteacher.

All users are required to read and accept this Acceptable Use Policy and complete cyber security training on an annual basis, as a condition of the RPA cyber insurance.

Email Policy

Emails form part of the school and trust's corporate records and emails sent or received while on school business or using school facilities are the property of the school.

- Managers should ensure that staff use email in accordance with this policy.
- The sending and receipt of personal email messages is permitted as long as it does not interfere with work commitments.
- Personal home email accounts should not be used to conduct school business with the public or external organisations.
- Users must not set up 'automatic' forwarding arrangements for any messages from their work account to one outside the Trust, e.g. at home. Automatically sending school or trust emails to external accounts increases the risk of disclosure or interception.
- Each user is responsible for the context of all text, audio and images that they send. They should ensure that private emails cannot be mis-interpreted as the views of the school and do not contradict our policies or interests.
- No email or other electronic communications may be sent which misrepresents the sender as anyone else.
- The email service should not be used for transmitting, accessing, retrieving or storing any communications of a discriminatory or harassing nature or that are racist, offensive, obscene, pornographic, or sexually explicit. This applies to both business and personal use.
- The sending or forwarding of chain letters or other unauthorised mass mailings, regardless of the subject matter, is not allowed.
- Treat suspect email or that from a dubious source with caution. Do not reply or forward (even to ICT support) a message if there is any doubt. Similarly do not open attachments or click on web links on suspect emails, as this could activate computer viruses or other malicious processes.
- The sending of unwanted messages can constitute harassment. Careless use of language can lead to a bullying tone and can also be considered harassment.
- Do not send (or forward) email containing derogatory statements, potentially libellous, defamatory, comments likely to cause offence, gossip, hoaxes, or jokes to others inside or outside the school or Trust.
- Use shortcuts or hyperlinks wherever possible, instead of attaching documents to emails. Large attachments (i.e. over 5Mb) should be avoided.

Use of the Internet

Users are granted access to the internet for business purposes and light personal use. Users must ensure that they comply with the provisions set out in this policy.

- The school maintains an awareness of staff Internet usage.
- Access to gambling, pornographic sites and sites of a similar nature, is not allowed under any circumstances.
- School or Trust information which is intended for internal use only, must not be placed on a system or website that is publicly accessible via the Internet.
- Staff should only enter personal information, e.g. credit card numbers, log in passwords etc. to websites if access to the site is encrypted, i.e. a 'padlock' symbol is shown in the bottom corner of the screen.
- The Internet is an insecure medium, therefore confidential or sensitive documents should only be sent by methods agreed to be secure. Guidance can be sought from the school office.
- It can be difficult to verify the true identity of a third party on the Internet. For your own safety and security and to protect the school and trust, information should not be shared with other users unless their identity is certain.
- Care must be taken using Social Networking sites in and out of work. The same care must be taken when posting information as sending email or writing official letters (see S*ocial Media Policy*).
- The School does not accept liability for any loss or damage arising from use of the Internet to make personal financial transactions.

Password and Security

Passwords protect information against accidental or malicious disclosure, modification or destruction. Information is an important and valuable asset which must be managed with care.

Users should follow good password practices. Passwords should:

- Be at least eight characters in length.
- Consist of a combination of lower case letters, upper case letters, numbers and special characters.
- Not contain two of the same characters consecutively.

- Be difficult for anyone else to guess.
- Be kept confidential and not shared with anyone, not written down, and not included as part of an automated routine e.g. stored in a macro.
- Be changed every 90 days and not used again for at least 12 months

Users must 'log out' of systems fully or use the CTRL+ALT+DEL 'lock computer' command when leaving a workstation unattended.

A short cut is to press the windows key+L

The school office ensures that staff have appropriate system access rights to undertake their roles, and that when an employee leaves or moves from their department that their system access rights are revoked.

School Devices and Mobile working

Mobile working, whether at home or away from normal business locations, brings with it additional threats to data security. Mobile equipment is also more vulnerable to theft, loss or unauthorised access.

While the other provisions of this policy apply equally when working on school data or equipment while outside school premises, additional requirements apply to school devices e.g. mobile phones, laptop and desk-top PCs.

- The device is the property of the school and issued to employees for the purpose of conducting school business. It is only for the use of the school employee to whom it is assigned.
- The devicemust be brought in to school during regularly scheduled work days in order to receive administrative communications, upgrades to anti-virus and other software.
- The devicemay be taken home or to other locations during and after school hours by the employee.The deviceis to be used for school work. Please see 'personal use' section for any use not related to school work. This will be monitored by ICT support.
- Data of a personal nature (such as school reports, pupil plans, photographs, etc.) can be accessed from home using remote access to the server or the use of OneDrive/Sharepoint. Memory sticks or other storage devices are blocked. It

must be recognised that this data comes under the UK General Data Protection Regulations and is subject to the trust's data protection policy.

- The equipment is issued to you in your current role. If your employment ends or you change schools or are on long term leave, the devicemust be handed back to the school office.
- Any costs generated by the user at home, such as phone bills, internet connection, printer cartridges, etc. are the responsibility of the user.
- The school office maintains records for the booking out of equipment.
- Always ensure that equipment and media are powered off when left unattended and preferably locked away.
- Equipment must be carried as hand luggage when travelling. If carried by vehicle, the equipment must be locked out of sight. It should not be left in an unattended vehicle, even if locked out of sight, for any length of time e.g. overnight.
- Any losses must be reported to the school immediately.
- Ensure that only equipment belonging to the school is connected to the school network.
- Any work saved onto laptops will be deleted automatically and will not be recoverable.

Personal Devices

School staff should not bring their personal devices to school for business use. The school cannot guarantee that personal devices have the same level of encryption, anti-virus and malware protection as school devices.

Staff should not store any student data or confidential information on their personal devices. Personal data should only be transferred to a home device if this is necessary for the member of staff to carry out their role.

When sending confidential information, staff must never save confidential information to a personal or household device. Data that is transferred from a work to a home device will be encrypted so that if any data is lost, stolen or subject to unauthorised access, it will remain safe until it can be recovered.

To ensure reasonable precautions are taken when managing data, staff will avoid:

- Keeping personal data on unencrypted hard drives.
- Sending work emails to and from personal email addresses.
- Leaving logged-in devices and files unattended.
- Using shared home devices where other household members can access personal data.

- Using an unsecured Wi-Fi network.

Staff working from home will be encouraged and enabled to go paperless, where possible, as paper files cannot be protected digitally and may be misplaced. If sensitive data is taken off the school premises to allow staff to work from home, it will be transported in a lockable bag or container. The school's procedures for taking data off the school premises will apply to both paper-based and electronic data.

Mobile Phones

- Staff should not use personal mobile phones when supervising children
- Staff must use a school phone when contacting parents. If a personal mobile has to be used make sure your number is withheld by typing the numbers 141 before you dial the number.
- Staff are advised not to share personal phone numbers with parents or pupils.
- Mobile phones are kept on the school premises at the owner's own risk. They should be switched off or set to silent mode during school hours.
- Any visitors to the school should be made aware of this policy and not use their mobiles in school.

The provisions above also apply to "smart" watches and glasses.

Photography

The regular use of iPad cameras and digital cameras for recording children's work or capturing special moments is encouraged for evidence and for promoting enjoyment. See the Data Protection policy for more information.

- All photos must be for professional use and not for personal use.
- For inclusion reasons, when possible and necessary, photos should be of groups of children rather than individuals.
- All users should take care to only take photos of an appropriate nature which cannot be misconstrued.
- With parental permission, photos can be added to the school website and its associate websites. It should not be possible to identify individual pupils by the use of their names.
- Photos should be stored on school equipment only not on personal devices.
- If any photos are taken on personal devices (e.g. whilst on educational visits) these must be transferred to a school device as soon as possible and then deleted from the personal device.
- Photos must not be given to any person outside school without the parents' express permission
- Where the person publishing material suspects that there may be child protection issues at stake, then serious consideration must be taken as to whether that material may be published or not.

Software and Virus protection

The Trust and its schools adhere strictly to software licence agreements.

- Staff should not load any software onto the school systems or school laptops.
- Users should not copy software nor use unlicensed copies of software.
- Care should be taken to prevent and detect the introduction of viruses and other malicious software by adhering to this policy. As such, USB devices are blocked on the school network. Users should instead save files to Sharepoint or Onedrive which can be accessed from anywhere with an internet connection.

However, if you suspect a virus on any School equipment:

- Inform the school office so that the school's ICT contractor can be informed.
- Unplug the network cable to isolate the PC
- Prevent anyone from using the PC.

Readable Information

Information from ICT systems is made readable on printed reports and computer display screens

- Schools should ensure that, where the public have access to the school buildings, computer screens are located out of the view of the public in order to protect confidential or sensitive information.
- Users should make sure that when using a mobile phone or laptop away from the office including use at home (especially on virtual meetings), that unauthorised individuals are not able to view or overhear confidential or sensitive information.
- Sensitive or critical business information should be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially outside working hours.
- Prints of sensitive information should be cleared from printers immediately.
- Where a printer is not within the view of the user, it is recommended that, where possible, "locked" or secure printing is used, i.e. it is necessary to enter a code or user name into the printer before the document is printed.

Personal Use

The school recognises that there are times when you may want to use the Systems for non-work related purposes, and in recognising this need the school permits you to use the Systems for personal use.

However, you must not allow personal use of Systems to interfere with your day to day duties. Excessive non-job related use of the Systems may be subject to disciplinary action.

Please be reminded that the internet and email service should not be used for transmitting, accessing, retrieving or storing any communications of a discriminatory or harassing nature or that are racist, offensive, obscene, pornographic, or sexually explicit. This applies to both business and personal use and is not allowed under any circumstances. Failure to adhere to this will result in disciplinary action

As mentioned above, all school Systems, including the external email system and internet usage may be monitored from time to time to ensure that the system is not being abused, to ensure that this policy is being complied with and for any other lawful purpose.

You are responsible for any non business-related files which are stored on your computer.

Ownership Rights

You should note that all information and files created, received, stored or sent by you while on school business or using school facilities form part of the school/trust's records and remain property of the school/trust.

Health and Safety – Display Screen Equipment Regulations

All employees have responsibility for Health & Safety in the workplace, and this will be reflected in the manner that IT is used. Employees and Managers are expected to ensure that the use of technology in their areas complies with the provisions of Health and Safety legislation and that the presence of technology in their work area is not a cause for concern.

There are specific requirements for Display Screen Equipment (DSE) users and, so far as the school is concerned, an employee falls within the requirements of the DSE regulations if they use equipment for continuous spells of an hour or more (on average) every day. Any such employees are required to complete a DSE risk self- assessment every 3 years. Risk assessment forms will be sent to you by the office, but additional advice and guidance can be found at: https://www.hse.gov.uk/pubns/ck1.pdf

Harassment and Abuse

The use of technology to harass and abuse others will not be tolerated. The trust has a clear and fundamental commitment to equal opportunities and the welfare of its employees and will not tolerate harassment in any form. This commitment is made explicit in the 'Dignity at Work Policy' which can be obtained from the school office.

Any employee found to be using technology as a means of harassing others will be investigated and disciplinary action will be taken as appropriate. This applies whether it is another employee or a member of the public who is subject to the harassment or abuse.

If an employee experiences harassment in any way they are urged to contact the Headteacher or Chair of Governors for advice and assistance.

Disciplinary Implications

The trust, school and Apex Network Solutions, reserve the right to inspect any files to ensure compliance with this policy. Access to internet sites may be logged and the data used by Apex Network Solutions and Headteachers for periodic review of access authorisations and usage.
Any misuse by pupils or staff should be reported to the Headteacher,

Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the Computer Misuse Act 1990, and may lead to prosecution of the school and the individual(s) concerned and/or civil claims for damages.

Appendix 1 - Pupil Acceptable Use Agreements

Schools may wish to use one of the following agreements with pupils:

Foundation Stage / KS1

At xxx School we know that it can be fun to use technology as part of your learning experience. We want everyone to be able to use technology, like computers and tablets, but it is important that you are safe when you are using them.We have created this agreement to help you understand how to be safe when you are using technology. Please read this carefully and sign your name to show that you understand your responsibilities when using technology. Ask your teacher if there is something that you do not understand.

I will:

- ✓ Only use technology, such as a computer, when a teacher has given me permission.
- ✓ Only use technology for the reason I have been asked to use it.
- ✓ Only use the internet when a teacher has given me permission.
- ✓ Ask for help when I have a problem using the technology.
- ✓ Look after the device and try not to damage it.
- ✓ Tell the teacher if my device is not working or damaged.
- ✓ Tell the teacher if I think someone else is not using technology safely or correctly.
- ✓ Tell the teacher if I see something online that I think is inappropriate or that makes me upset.

I will not:

- × Tell another pupil my username and password.
- × Share personal information, such as my age and where I live, about myself or my friends online.
- × Access social media, such as Facebook and WhatsApp.
- × Speak to strangers on the internet.
- × Take photos of myself or my friends using a school device unless my friend and an adult in school has agreed and the photo/video is appropriate.

KS2

This is how we stay safe when we use computers:

I understand that the school will monitor how I use technology

I will only use technology for activities that a teacher or adult has told or allowed me to use

I will take care of the computer and other equipment

I will keep my usernames and passwords safe and secure

I will not share personal information about myself or others when on-line

I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong

I will be polite and responsible when I communicate with others

I will not use my own devices in school, unless I have permission

I know if I break the rules I might not be allowed to use a computer or tablet

Please read each statement and provide a tick to show that you agree, and then write your name below.

- ☐ I understand why it is important to use technology safely and correctly.
- ☐ I understand my responsibilities when using technology.
- ☐ I understand that I may not be allowed to use technology if I do not use it safely and correctly.
- ☐ I will follow these rules at all times.

Pupil name (please print): _____

Date: _____

Parent name (please print): _____

Parent signature: _____

Date: _____