# IT POLICY - (including Social Media)

**Document Owner:** ICT Network Director
**Date:** January 2026
**Status:** Non-statutory

City Learning Trust
Inspiring Outstanding Achievement

To ensure you are always referencing the most current version, where possible **DO NOT** download a copy of this document.

If a paper copy is required please print and destroy as soon as possible.

**DO NOT** save a copy to your own device/desktop.

## TABLE OF CONTENTS

# 1. POLICY STATEMENT

a. Information and Communications Technology (ICT) in the 21st Century is an integral part of the way our Academy works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of our schools and the Trust. ICT covers a wide range of resources including web-based and mobile learning. It is important to recognise the constant and fast paced evolution of ICT within our society as a whole. Our pupils and staff have access to ICT and whilst exciting and beneficial both inside and outside of the classroom, we are also aware that the ICT resources and facilities our schools use could also pose risks to data protection, online safety and safeguarding.

b. This policy aims to:

i. Set guidelines and rules on the use of Academy ICT resources for staff, pupils, Parents/Carers and governors
ii. Establish clear expectations for the way all members of the Academy community engage with each other online
iii. Support the Academy's policies on data protection, behaviour and safeguarding
iv. Prevent disruption that could occur to the Academy through the misuse, or attempted misuse, of ICT systems
v. Support the Academy in teaching pupils safe and effective internet, social media and ICT use
vi. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

c. This policy covers all users of our Academy's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors. Breaches of this policy may be dealt with under our Disciplinary Policy, Behaviour Policy or Code of Conduct.

# 2. RELEVANT LEGISLATION AND GUIDANCE

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

i. Data Protection Act 2018
ii. The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
iii. Computer Misuse Act 1990
iv. Human Rights Act 1998
v. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
vi. Education Act 2011
vii. Freedom of Information Act 2000
viii. Education and Inspections Act 2006
ix. Keeping Children Safe in Education 2024
x. Searching, screening and confiscation: advice for Academies 2022
xi. National Cyber Security Centre (NCSC): Cyber Security for Academies x
xii. Education and Training (Welfare of Children) Act 2021
xiii. UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
xiv. Meeting digital and technology standards in Academies and colleges
xv. The Policy also considers the National Curriculum Computing Programmes of Study.
xvi. This Policy complies with our funding agreement and articles of association.

# 3. DEFINITIONS

## 3.1 ICT Facilities

a. All facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future and is provided as part of the Academy's ICT service.

## 3.2 Users

a. Anyone authorised by the Academy to use the Academy's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

## 3.3 Personal Use

a. Any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user.

## 3.4 Authorised Personnel

a. Employees authorised by the Academy to perform systems administration and/or monitoring of the ICT facilities.

## 3.5 Materials

a. Files and data created using the Academy's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

b. See Appendix E for a glossary of cyber security terminology.

# 4. UNACCEPTABLE USE

a. The following is considered unacceptable use of the Academy's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 5.2 below).

b. Unacceptable use of the Academy's ICT facilities includes:
   i. Using the Academy's ICT facilities to breach intellectual property rights or copyright
   ii. Using the Academy's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
   iii. Breaching the Academy's policies or procedures
   iv. Any illegal conduct, or statements which are deemed to be advocating illegal activity
   v. Online gambling, inappropriate advertising, phishing and/or financial scams
   vi. Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
   vii. Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
   viii. Activity which defames or disparages the Academy, or risks bringing the Academy into disrepute
   ix. Sharing confidential information about the Academy, its pupils, or other members of the Academy community
   x. Connecting any device to the Academy's ICT network without approval from authorised personnel
   xi. Setting up any software, applications or web services on the Academy's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the Academy's ICT facilities, accounts or data
   xii. Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
   xiii. Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the Academy's ICT facilities
   xiv. Causing intentional damage to the Academy's ICT facilities
   xv. Removing, deleting or disposing of the Academy's ICT equipment, systems, programmes or information without permission from authorised personnel
   xvi. Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
   xvii. Using inappropriate or offensive language
   xviii. Promoting a private business, unless that business is directly related to the Academy
   xix. Using websites or mechanisms to bypass the Academy's filtering or monitoring mechanisms
   xx. Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way.

c. This is not an exhaustive list. The Academy reserves the right to amend this list at any time. The Headteacher / Principal will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Academy's ICT facilities.

## 4.1 Exceptions From Unacceptable Use

a. Where the use of Academy ICT facilities (on the Academy premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher/ Principal's discretion. Please contact the Headteacher/Principal to discuss further.

## 4.2 Sanctions

a. Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Academy's policies on Behaviour / Discipline / Code of Conduct. Copies of these policies can be found on our website or on request through the Academy Admin Team.

# 5. STAFF

(Including Governors, Volunteers, and Contractors)

## 5.1 Access to Academy ICT facilities and materials

a. The Trust ICT Network Director manages access to the Academy's ICT facilities and materials for Academy staff. That includes, but is not limited to:
   i. Computers, tablets, mobile phones and other devices
   ii. Access permissions for certain programmes or files

b. Staff will be provided with unique login/account information and passwords that they must use when accessing the Academy's ICT facilities. Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Trust ICT Network Director. Where appropriate, multi-factor authentication will also be required.

## 5.2 Laptop Agreement For Staff

a. The laptop is issued to you for the following purposes:
   i. To access your email
   ii. To complete online registration and reports
   iii. To support teaching and learning, including the use of the VLE and other supportive software

b. You will be responsible for the security of the confidential information which can be accessed by or stored on your machine. All sources of such data should be protected by a secure password (minimum of 8 characters including at least one letter and one number) and must be protected from the sight of students or the possibility of unauthorised access (see Data Protection Policy for more information).

c. The school's insurance policy covers the laptop against theft whilst it is in school, provided it is not left unattended.

d. Further information regarding staff laptop agreement and use can be found in Appendix F.

## 5.3. Use of Phones, Email/Internet And Audio Visual Equipment

### 5.3.1 Email / Internet Resources

a. The Academy provides each member of staff with an email address. This email account should be used for work purposes only to support in the interchange of information, the enhancement of lessons and to provide opportunities to share resources and facilitate collaboration through electronic communication and networking. All work-related business should be conducted using the email address the Academy has provided. Staff must not share their personal email addresses with Parents/Carers and pupils, and must not send any work-related materials using their personal email account. Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

b. Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018, in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable and not private.

c. Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. Staff MUST check addresses they are using are correct/accurate.

d. If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. The Data Protection Officer must be advised.

e. If staff send an email in error that contains the personal information of another person, they must inform their Headteacher/Principal and the Data Protection Officer immediately and follow our data breach procedures.

f. The internet provides the Trust with the means to send information to, receive information from, and access resources outside the company's network. As with all internal email messages, messages can be forwarded without the knowledge or consent of the original author. Users, therefore, must exert caution in the transmission of messages outside the Trust and must comply with any appropriate legislative requirements. All emails must hold a signature which states the CLT disclaimer.

### 5.3.2 Prohibited Purposes of Email/Internet Use

a. Personal use in working hours must be limited, personal use creating a direct cost for the Trust is prohibited.

b. Use at any time for personal monetary gain or for commercial purposes that are not directly related to the Trust.

### 5.3.3 Other Prohibited Uses

a. Other prohibited uses of email/internet resources include but are not limited to:
   i. Inclusion of the work of others into electronic communications in violation of copyright laws
   ii. Use of the internet to harass or intimidate others, or to interfere with the ability of others to conduct CLT business
   iii. Use of the internet for any purpose that is restricted or prohibited by laws or regulations
   iv. 'Spoofing' – constructing electronic communication in such a way that it appears to be from someone else
   v. 'Snooping' – obtaining access to the files or electronic mail of others for the purpose of satisfying idle curiosity with no substantial purpose
   vi. Attempting to breach security measures on any internal or external system
   vii. Attempting to intercept electronic communications without authorisation
   viii. Use of bulletin or notice boards for personal advertising or any non-business purpose
   ix. Accessing, sending or receiving or storing information or pictures with pornographic or paedophilic content
   x. Accessing, sending or receiving or storing information or pictures of a sexually or racially discriminating nature
   xi. Accessing, sending or receiving or information of a defamatory or libellous nature about any person or organisation

### 5.3.4 Trust Access And Disclosure

a. The content of all email messages received or sent by employees of the Trust and stored on any server, or other resource or equipment shall be deemed to be the property of the Trust. To the extent permitted by law, the Trust reserves the right to access and disclose any person's use of the internet or the contents of any user's electronic mail without the consent of the user. The Trust will do so when it believes it has legitimate business need and only after explicit authorisation is gained from a Trustee and HR.

b. All members of staff are advised that the Trust's electronic mail systems should be treated like a filing system i.e. with the expectation that communications sent and received on company business may be made available for review by any Trustee.

c. Many email messages are in the category of temporary or non-vital and should be discarded routinely. Where the message is of great importance and requires retention for future reference it should be copied to secure storage (or printed and filed) and removed from the email system.

### 5.3.5 Monitoring of Communications

a. The Trust reserves the right to monitor internet access and email usage as a routine matter, to the extent permitted by law. To this end, all in bound and out bound internet activity, including emails and their contents, are logged and regularly reported on. When using internet services, as provided by the Trust, you agree to the monitoring and logging of all internet communications.

### 5.3.6 Inspections and Disclosure of Communication

a. To the extent permitted by law, the Trust reserves the right to access and disclose any person's use of the internet or the contents of any user's electronic mail without the consent of the user.

b. In the course of an investigation triggered by indications of misconduct or misuse the contents or subjects of all internet access may be disclosed.

c. The Trust will inspect and disclose the subject of internet access when such action is necessary to respond to legal processes and to fulfil the Trust's obligations to third parties.

### 5.3.7 Limitations on Disclosure and Use of Information obtained by means of Access or Monitoring

a. The content of electronic mail communications or internet downloads, properly obtained for Trust purposes may be disclosed without permission of the user. The Trust will attempt to refrain from disclosure of particular communications if the disclosure appears likely to cause personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

### 5.3.8 Special Procedures to approve access to, disclosure of, or use of electronic mail communications

a. Individuals requiring access to electronic mail communications of others, to use the information gained from such access and who do not have consent of the user must obtain approval by a Trustee and HR.

### 5.3.9 Cessation of Employment or Transfer

a. Employees whose employment ceases for any reason or who are laid off have no right to the contents of their email messages and no right to access the email system.

### 5.3.10 Potential Risks to the System and Business

a. All users of the internet gateway should be aware of, and take steps to avoid the following potential risks to the Trust's systems or business:
   i. The possibility of inadvertently constituting a binding contract through completion of an online agreement form or exchange of email messages.
   ii. Electronic messages submitted to third parties should be treated in the same way as any other written or email communication, and be subject to the same controls and authorisations
   iii. The introduction of a virus onto the CLT network – files must not be downloaded or copied from any internet site without approval.
   iv. City Learning Trust considers any violation of this policy as a serious offence which will be dealt with under the Trust's disciplinary Policy.

## 5.4 Mobile Phones

a. Staff are permitted to bring in personal mobile phones for their own use during non-contact time and out of sight of all pupils.

b. Staff must not give their personal phone number(s) to Parents/Carers or pupils.

c. Staff must where possible use phones (landlines and mobiles) provided by the Academy to conduct all work-related business. If a personal phone must be used, 141 must be pressed before the telephone number to ensure your personal phone number remains private.

d. Staff who are provided with mobile phones as equipment for their role, must abide by the same rules for ICT acceptable use as set out in section 5.

e. The sending of inappropriate text messages, explicit photographs, video/audio recordings of defamatory or derogatory nature between any member of the Trust community (including outside of school hours) is prohibited and such conduct may be subject to disciplinary and/or criminal investigation as appropriate.

f. The Academy is not responsible for the loss, damage or theft of any personal mobile device.

g. Users bringing personal devices into Academy must ensure there is no inappropriate or illegal content on the device.

## 5.5 Walkie Talkies

a. The use of Walkie Talkies/Two way radios within our Academies is recognised as being an important method of communication, to ensure the safety and well-being of our students and staff. How Walkie Talkies are used to communicate and the nature of the information being communicated is an important part of keeping children safe.

b. Walkie Talkies are used by staff within school to request assistance. This could be with regard to daily operational needs, such as requesting support of a site supervisor for a maintenance activity. However, there are occasions when assistance may be required for a pupil/member of staff in relation to an accident or medical condition, or another urgent need scenario on the site and it is important the appropriate assistance is received as swiftly as possible.

### 5.5.1 Walkie Talkie Data Protection

a. It is important to understand that when communicating information via a walkie-talkie, you are communicating over a radio network. Therefore, others in the vicinity using the same network may also be able to hear your conversations e.g. taxi drivers. Therefore, it is important that appropriate controls are in place.

b. Article 5 (1) (f) of the General Data Protection Regulation requires that personal data should be:

   i. 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality)'.

### 5.5.2 Risks/Consequences

a. To minimise the risk of unauthorised access to any information that is communicated via Walkie Talkies, we apply the best practice recommendations below to prevent individuals without the correct authorisation intentionally or accidentally gaining access to personal information.

b. Any unauthorised access to information may result in a safeguarding issue or a Data Protection breach.

c. Any suspected personal data breach should be reported to the Academy Headteacher/Principal and to the City Learning Trust Data Protection Officer.

### 5.5.3 Training

a. City Learning Trust advocates the undertaking of the 'Information Governance and Data Security' online training. Please contact HR for more information regarding this online training.

### 5.5.4 Best Practice - Conduct expected when using Walkie-Talkies

a. Under no circumstances must any personal information be communicated which could enable an individual to be identified. For example, only communicate first name or initials or use a code system when requesting assistance.

b. Each member of staff is required to ensure the safety of their Walkie Talkie. In the event of loss due to a theft or item being lost, the member of staff must inform the Headteacher/Principal and Data Protection Officer as soon as possible.

c. The member of staff is obligated to ensure that the communication language used on the Walkie Talkie is professional and under no circumstances must they use abusive or inappropriate language.

d. The units must be signed out to staff. The units are only to be used for professional use around the Academy. Under no circumstances are they used for personal/casual conversations.

e. Content of the communications must be confidential, respecting data protection, safeguarding and privacy.

f. Radios/walkie-talkies should never be given to a student to use.

g. In conjunction with this policy, the City Learning Trust Data Protection Policy should be read and understood by all staff. This is available on the Academy website.

### 5.5.5 Personal Use

a. Staff are permitted to use Academy ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Trust ICT Network Director may withdraw or restrict this permission at any time and at their discretion in consultation with the Headteacher/ Principal of the Academy.

b. Personal use is permitted provided that such use:
   i. Does not take place during the academic working day when pupils are present
   ii. Does not constitute 'unacceptable use', as defined in section 5
   iii. Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

c. Staff may not use the Academy's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

d. Staff should be aware that use of the Academy's ICT facilities for personal use may put personal communications within the scope of the Academy's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

e. Staff should be aware that personal use of ICT (even when not using Academy ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and Parents/Carers could see them.

f. Staff should take care to follow the Academy's guidelines on the use of social media (see Appendix A and use of email (see Section 6.3.1) to protect themselves online and avoid compromising their professional integrity.

## 5.6 Personal Social Media Accounts

a. Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. Only authorised personnel are permitted to use Social Media on behalf of the Trust or Academy (please see Section 10 below).

b. The Academy has guidelines for staff on appropriate personal security settings for Facebook and other Social Media accounts (see Appendix A).

## 5.7 Using Your Own Device (UYOD) for Work Purposes

a. Personal devices such as laptops, ipads, cameras, USB devices/hard drives can be useful to support the teaching and learning taking place within the Academy. However, the use of such devices to create and process Trust information and data creates issues that need to be addressed, particularly with regard to information security.

b. The Trust must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. We must also protect its intellectual property as well as empowering staff to ensure that they protect their own personal information.

c. All relevant Trust and Academy policies apply to staff using their own devices including the Data Protection Policy.

d. Individuals who make use of UYOD must take responsibility for their own device and how they use it.

e. They must:
   i. Inform the ICT Network Director of their intention to use their own device, before bringing this on site.
   ii. Familiarise themselves with their device and its security features so that they can ensure the safety of Trust information (as well as their own information).
   iii. Invoke the relevant security features.
   iv. Maintain the device themselves, ensuring it is regularly patched and upgraded.
   v. Ensure that the device is not used for any purpose that would not be compliant with this Policy.
   vi. While City Learning Trust IT employees will always endeavour to assist colleagues wherever possible, the Trust cannot take responsibility for supporting devices it does not provide.

f. Employees using their own devices must take all reasonable steps to:
   i. Prevent theft and loss of data.
   ii. Keep information confidential where appropriate.
   iii. Maintain the integrity of data and information, including that on CLT sites
   iv. Take responsibility for any software they download onto their device.

g. Employees using their own devices must:
   i. Allow the ICT Network Director to place on the device any form of monitoring management for the purpose of safeguarding children such as SENSO cloud.
   ii. Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device.
   iii. Set up remote wipe facilities if available and implement a remote wipe if they lose their device.
   iv. Encrypt documents or devices as necessary - IT Support team members can help with this if necessary.

v. Not hold any information that is sensitive, personal, confidential or of commercial value on personally owned devices.
vi. Where it is essential that information belonging to the Trust is held on a personal device it should be deleted as soon as possible once it is no longer required. This includes information contained within emails.
vii. Ensure that relevant information is copied back onto Trust systems and manage any potential data integrity issues with existing information.
viii. Report the loss of any devices containing Trust data (including email) to the Data Protection Officer.
ix. Be aware of any Data Protection issues and ensure personal data is handled appropriately.
x. Report any security breach immediately to the Data Protection Officer and ensure personal data is handled appropriately.
xi. Ensure that no Trust information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party.
xii. Academy staff may only use personal devices (including computers and USB drives) to access Academy data, work remotely, or take personal data (such as pupil information) out of the Academy if they have been specifically authorised to do so by the Headteacher/Principal.
xiii. Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT Network Director.

# 6. ROLES AND RESPONSIBILITIES

## 6.1 The Local Governing Committee

a. The Local Governing Committee in each Academy has overall responsibility for monitoring this policy and holding their respective Headteacher/Principal to account for its implementation.

b. The Local Governing Committee will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL) for each Academy.

c. There is a named Trustee who oversees online safety within the Trust. There is a named Governor in each Academy who oversees safeguarding, including online safety.

d. All Trustees and Governors will:
   i. Ensure that they have read and understand this policy
   ii. Agree and adhere to the terms on acceptable use of the Academy's ICT systems and the internet

## 6.2 The Headteacher/Principal

a. The Headteacher/Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Academy.

## 6.3 The Designated Safeguarding Lead

a. Details of the Academy's Designated Safeguarding Lead (DSL), Deputy and Safeguarding Officers are set out in our child protection and Safeguarding policy.

b. The DSL takes lead responsibility for online safety in the Academy, in particular:

c. Supporting the Headteacher/Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy

d. Working with the Headteacher/Principal, ICT Network Director and other staff, as necessary, to address any online safety issues or incidents

e. Ensuring that any online safety incidents are logged on CPOMS (or other Academy recording method) and dealt with appropriately in line with this policy

f. Ensuring any incidents of cyber-bullying are logged and dealt with appropriately in line with Academy behaviour policy

g. Updating and delivering staff training on online safety

h. Liaising with other agencies and/or external services if necessary

i. Providing regular reports on online safety, to the Headteacher/Principal and/or Local Governing Committee

j. This list is not intended to be exhaustive.

## 6.4 The ICT Network Director

a. The ICT Network Director is responsible for:
   i. Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online, whilst at the Academy and using Academy equipment, including terrorist and extremist material
   ii. Ensuring that the Academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
   iii. Conducting regular security checks and monitoring the Academy's ICT systems.
   iv. Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
   v. Ensuring any online safety incidents are logged on CPOMS (or relevant recording procedures) and dealt with appropriately in line with this policy
   vi. Ensuring any incidents of cyber-bullying are dealt with appropriately in line with the Academy Behaviour Policy.

b. This list is not intended to be exhaustive.

## 6.5 Staff and Volunteers

a. All staff, including contractors and agency staff, and volunteers are responsible for:
   i. Maintaining an understanding of this policy. **Please note:** Social Media guidelines and protocols are also included as a key appendix – Appendix A.
   ii. Implementing this policy consistently
   iii. Agreeing and adhering to the terms on acceptable use of the Academy's ICT systems and the
   iv. internet, and ensuring that pupils follow the Academy's terms on acceptable use
   v. Working with the DSL to ensure any online safety incidents are logged and dealt with appropriately in line with this policy
   vi. Ensuring that any incidents of cyber-bullying are recorded and dealt with appropriately in line with the Academy behaviour policy.

b. This list is not intended to be exhaustive.

## 6.6 Parents/Carers

a. Parents/Carers are asked to:
   i. Notify a member of staff or the Headteacher/Principal of any concerns or queries regarding this policy
   ii. Ensure their child has read, understood and agreed to terms on acceptable use of Academy's ICT systems/ internet

b. Parents/Carers can seek guidance on keeping children safe online from following the organisations and websites:
   i. What are issues?, UK Safer Internet Centre: https://saferinternet.org.uk/guide-and-resource/ what-are-the-issues
   ii. Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
   iii. Visitors and Members of the Community

c. Visitors and members of the community who use the Academy's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

# 7. MONITORING AND ACCESS

a. The Trust reserves the right to:
   i. Monitor a personal device in line with our monitoring management procedures and processes for safeguarding, such as SENSO Cloud.
   ii. Prevent personal devices being used on site if monitoring management procedures are denied.
   iii. Prevent access to either the wired or wireless networks or both.
   iv. Prevent access to a particular system.
   v. Take all necessary and appropriate steps to retrieve information owned by the Trust.

## 8. DATA PROTECTION AND UYOD

a. The Trust and Member Academies must process 'personal data', that is data about identifiable living individuals in accordance with the Data Protection Act 1998. Sensitive category, personal data, is information that relates to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (mental or physical) or details of criminal offences. This category of information should be handled with a higher degree of protection at all times.

b. The Trust and Member Academies, in line with the guidance from the Information Commissioner's Office on use of own devices, recognises that there are inherent risks in using personal devices to hold personal data and where possible, it is recommended that staff do not use their own personal devices for work purposes.

c. A breach of the Data Protection Act can lead to the Trust receiving a substantial fine. Any member or employees found to have deliberately breached the Act may be subject to disciplinary measures, having access to the Trust and Member Academies facilities being withdrawn, or even criminal prosecution.

## 9. REMOTE ACCESS

a. We allow staff to access the Academy's ICT facilities and materials remotely. Staff accessing the Academy's ICT facilities and materials remotely, must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the Academy's ICT facilities outside the Academy and take precautions against importing viruses or compromising system security.

b. Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy. Further information is within our Data Protection Policy.

### 9.1 Remote Teaching / Online Parents' Evenings and Online Lessons or Communication

a. Remote provision will only take place using systems which have been assessed by the ICT Network Director.

b. Employees will only use managed or specific, approved professional accounts with learners, Parents/ Carers.

c. Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.

d. All remote lessons will be formally timetabled; Online Admin can 'drop in' at any time.

e. Any personal data used by employees and captured when delivering remote learning will be processed in accordance with our data protection policy (please see our GDPR policy).

f. All participants will be made aware that remote learning systems will be recorded and monitored closely.

g. Employees will not record lessons or meetings using personal equipment unless agreed and this is risk assessed by the ICT Network Director and approved by the Executive Leadership Group as in line with our Data Protection Policy.

## 10. ACADEMY SOCIAL MEDIA ACCOUNTS

a. The Academy and the Trust have official social media accounts, managed by The Trust ICT Network Director. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account. The Academy has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times. Social Media accounts must not be created by members of staff to advertise their subject/ sports or other Academy work. Only official accounts are to be utilised.

## 11. MONITORING AND FILTERING OF THE ACADEMY NETWORK AND USE OF ICT FACILITIES

a. To safeguard and promote the welfare of children and provide them with a safe environment to learn, the Academy reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:
   i. Internet sites visited
   ii. ii.Bandwidth usage
   iii. iii.Email accounts iv.Telephone calls

b. User activity/access logs

c. Any other electronic communications

d. Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The effectiveness of any filtering and monitoring will be regularly reviewed.

e. Where appropriate, authorised personnel may raise concerns about monitored activity with the Academy's Designated Safeguarding Lead (DSL) and ICT Network Director as appropriate.

f. Please note that during personal communications using the Academy ICT, this communication may also be unavoidably included in any business communications that are monitored as above.

g. The Academy monitors ICT use in order to:
   i. Obtain information related to Academy business
   ii. Investigate compliance with Academy policies, procedures and standards
   iii. Ensure effective Academy and ICT operation
   iv. Conduct training or quality control exercises
   v. Prevent or detect crime
   vi. Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

# 12. PUPILS

## 12.1 Access to ICT Facilities

a. Pupils have access to computers and equipment in the Academy for the purpose of accessing learning materials.

b. Specialist ICT equipment, such as that used for Music or Design and Technology, must only be used under the supervision of staff.

c. Pupils will be provided with a unique user email address and protected password for the use of school communications or uploading of work to their teacher.

d. Pupils will be provided with accounts linked to Academy virtual learning environments, for the purpose of accessing learning materials.

e. Pupils are expected to adhere to this policy and not breach any of the points raised in section 5 pertaining to unacceptable use. Failure to do so, could result in sanctions being put in place under the Behaviour Policy.

## 12.2 Acceptable Use Agreement: Students

a. When using ICT equipment and facilities in the Academy you are agreeing to the following:
   i. I will only use ICT systems in the Academy, including the internet, e-mail, digital video, mobile technologies, etc. for School purposes.
   ii. I will not download or install software on School technologies.
   iii. I will only log on to the School network/ Learning Platform with my own user name and password.
   iv. I will follow the Schools ICT security system and not reveal my passwords to anyone and change them regularly.
   v. I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
   vi. I will be responsible for my behaviour when using the Internet; This includes resources I access and the language I use.
   vii. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal (this can include photographs, images, videos, emails, and sound clips).
   viii. If I accidentally come across any such material I will report it immediately to my Teacher, Tutor or Head of Year or Designated Safeguarding Lead.
   ix. I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a School project approved by my teacher.
   x. Images of Students and/or staff will only be taken with the permission of the person involved and will be stored and used for School purposes in line with School Policy. Images should not be distributed outside the School network without the permission of the Headteacher/Principal.
   xi. I will ensure that my online activity, both in School and outside School, will not cause my School, the staff, pupils or others distress or bring into disrepute the Academy.
   xii. I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the School community.
   xiii. I will respect the privacy and ownership of others' work on-line at all times.
   xiv. I will not attempt to bypass the internet filtering system.
   xv. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to appropriate staff.
   xvi. I understand that these rules are designed to keep me safe and that if they are not followed, School sanctions will be applied and my parent/ carer may be contacted.

b. Please refer to the Behaviour Policy for more information.

## 12.3 Search and Deletion

a. Under the Education Act 2011, the Headteacher/Principal, and any member of staff authorised to do so by the Headteacher/Principal, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting contain inappropriate images or files. The member of staff can delete these if necessary.

b. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:
   i. Cause harm/ pose a risk to staff or pupils, and/or
   ii. Disrupt teaching, and/or
   iii. Break any of the Academy rules
   iv. Is evidence in relation to an offence

c. This includes, but is not limited to:
   i. Pornography
   ii. Abusive messages, images or videos
   iii. Indecent images of children
   iv. Evidence of suspected criminal behaviour (such as threats of violence or assault)

d. If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the Senior Leadership Team to decide whether they should:
   i. Delete that material, or
   ii. Retain it as evidence (of a criminal offence or a breach of Academy discipline), and/or
   iii. Report it to the police

e. Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
   i. Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher/Principal or DSL.
   ii. Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
   iii. Seek the pupil's co-operation (not permission)

f. The authorised staff member should:
   a. Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.
   b. Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

g. Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

h. When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has, or could be used to:
   i. Cause harm, and/or
   ii. Undermine the safe environment of the Academy or disrupt teaching, and/or
   iii. Commit an offence

i. If inappropriate material is found on the device, it is up to the Headteacher/Principal to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

j. When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:
   i. They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
   ii. The pupil and/or the parent refuses to delete the material themselves

k. If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:
   i. **Not** view the image
   ii. **Not** copy, print, share, store or save the image
   iii. Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

l. Any searching of pupils will be carried out in line with:
   i. The DfE's latest guidance on searching, screening and confiscation
   ii. UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
   iii. Our behaviour policy / searches and confiscation policy
   iv. Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the Academy complaints procedure.

### 12.4 Unacceptable Use of ICT and the Internet Outside of Academy

a. The Academy will sanction pupils, in line with the Behaviour Policy, if a pupil engages in any of the following **at any time** (even if they are not on Academy premises):
   i. Using ICT or the internet to breach intellectual property rights or copyright
   ii. Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
   iii. Breaching the Academy's policies or procedures
   iv. Any illegal conduct, or making statements which are deemed to be advocating illegal activity
   v. Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
   vi. Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
   vii. Activity which defames or disparages the Academy, or risks bringing the Academy into disrepute
   viii. Sharing confidential information about the Academy, other pupils, staff or other members of the Academy community
   ix. Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
   x. Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to Academy's ICT facilities
   xi. Causing intentional damage to the Academy's ICT facilities or materials
   xii. Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/ or those they share it with are not supposed to have access, or without authorisation
   xiii. Using inappropriate or offensive language.

## 13. E-SAFETY EDUCATION

a. Pupils will be taught about online safety as part of their curriculum.

b. In Key Stage 1 and 2, pupils will be taught to:
   i. Use technology safely, respectfully and responsibly
   ii. Recognise acceptable and unacceptable behaviour
   iii. Identify a range of ways to report concerns about content and contact

c. In Key Stage 3 and 4, pupils will be taught to:
   i. Understand a range of ways to use technology safely, respectfully, responsibly and securely including protecting their online identity and privacy
   ii. Recognise inappropriate content, contact and conduct, and know how to report concerns

d. The safe use of social media and the internet will also be covered in other subjects where relevant.

e. The Academy will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

## 14. CYBER BULLYING

### 14.1 Definition

a. Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power (See also the Academy Behaviour Policy).

### 14.2 Preventing and Addressing Cyber-Bullying

a. To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

b. The Academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Tutors/ Teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

c. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

d. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

e. The Academy also sends information on cyber-bullying to Parents/Carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

f. In relation to a specific incident of cyber-bullying, the Academy will follow the processes set out in the Academy Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the Academy will use all reasonable endeavours to ensure the incident is contained and appropriately dealt with.

g. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

# 15. REMOTE LEARNING

## 15.1 Pupils

a. In order to support remote learning opportunities and online communication practices which are essential to the educational offer and Home/School Partnership, when accessing live lessons:
   i. Do not under any circumstances share the online platform invite with anyone who is not in your class.
   ii. Make sure that your screen name (the name that appears on the screen) is your real name. Any name that is not identifiable as someone in the class will not be admitted to the lesson.
   iii. Students will only be admitted into the online platform when there is a minimum of three participants.
   iv. Leave your camera on, so that we can see your face, this is for safeguarding purposes.

## 15.2 Parents/Carers

### 15.2.1 Access to ICT Facilities and Materials

a. Parents/Carers do not have access to the Academy's ICT facilities as a matter of course, however, Parents/Carers working for, or with, the Academy in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the Academy's facilities at the Headteacher/ Principal's discretion. Where Parents/Carers are granted access in this way, they must abide by this policy as it applies to staff.

### 15.2.2 Communicating with or about the Academy Online

a. We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online. Parents/Carers play a vital role in helping model this behaviour for their children, especially when communicating with the Academy through our website and social media channels.

b. We ask Parents/Carers to sign the agreement in Appendix B.

### 15.2.3 Communicating with Parents/Carers about Pupil Activity

a. The Academy will ensure that Parents/Carers and carers are made aware of any online activity that their children are being asked to carry out. When we ask pupils to use websites or engage in online activity, we will communicate the details of this to Parents/Carers in the same way that information about homework tasks are shared.

b. In particular, staff will let Parents/Carers know which (if any) person or people from the Academy pupils will be interacting with online, including the purpose of the interaction. Parents/Carers may seek any support and advice from the Academy to ensure a safe online environment is established for their child.

# 16. DATA SECURITY

a. The Academy is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

b. Staff, pupils, Parents/Carers and others who use the Academy's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in Academys and colleges, including the use of:
   i. Firewalls
   ii. Security features
   iii. User authentication and multi-factor authentication
   iv. Anti-malware software

## 16.1 Passwords and Password Security

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

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

c. Members of staff or pupils who disclose account or password information may face disciplinary action. Parents/ Carers, visitors or volunteers who disclose account or password information may have their access rights revoked. All staff will use the password manager required by the ICT Network Director to help them store their passwords securely. Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

d. Passwords are to be changed on a regular basis and prompts will be given through the computer network.

## 16.2 Passwords

a. Always use your own personal passwords to access computer based services

b. Make sure you enter your personal password each time you log-on. Do not include passwords in any automated log-on procedures

c. Staff and Students should change temporary passwords at first log-on

d. Change passwords whenever there is any indication of possible system or password compromise

e. Do not record passwords or encryption keys on paper or in an unprotected file

f. Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

g. User ID and passwords for staff and pupils who have left the Trust are disabled after their last day in the Trust.

h. If you think your password may have been compromised or someone else has become aware of your password report this to the ICT Network Director.

## 16.3 Password Security

a. Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. Where it is possible and appropriate to use multi-factor authentication, this will also be used.

b. All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the Trust's e-safety Policy and Data Security

c. Users are provided with an individual network, email, Learning Platform and Management Information System log-in username.

d. Pupils are not allowed to deliberately access on-line materials or files on the School network, of their peers, teachers or others

e. Staff are made aware of their individual responsibilities to protect the security and confidentiality of School networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

f. All staff and students are expected to comply with this policy at all times.

## 16.4 Software Updates, Firewalls and Anti-Virus Software

a. All of the Academy's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

b. Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the Academy's ICT facilities.

c. Any personal devices using the Academy's network must all be configured in this way.

## 16.5 Data Protection

a. All personal data must be processed and stored in line with data protection regulations and the Academy's Data Protection Policy.

## 16.6 Access to Facilities and Materials

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

b. Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert their Headteacher/Principal immediately.

c. Users should always log out of systems and lock their equipment when they are not in use, to avoid any unauthorised access. Equipment and systems (including IWBs) should always be logged out of and shut down completely at the end of each working day.

## 16.7 Encryption

a. The Academy makes sure that its devices and systems have an appropriate level of encryption for protection purposes.

# 17. PROTECTION FROM CYBER ATTACKS

a. Please see the glossary (Appendix E) for cyber security terminology.

b. The Academy will:
   i. Work with the ICT Network Director to make sure cyber security is given the time and resources it needs to make the Academy secure
   ii. Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the Academy's annual training window) on the basics of cyber security, including how to:
      - Check the sender address in an email
      - Respond to a request for bank details, personal information or log-in details
      - Verify requests for payments or changes to information

c. Make sure staff are aware of our procedures for reporting and responding to cyber security incidents

d. Investigate whether our IT software needs updating or replacing to be more secure

e. Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data

f. Put controls in place that are:
   i. **Proportionate**: the Academy will verify this annually, using a third-party audit, to objectively test that what it has in place is effective
   ii. **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
   iii. **Up to date:** with a system in place to monitor when the Academy needs to update its software
   iv. **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
   v. Back up critical data daily and store these backups on cloud based backup systems.

g. Make sure staff:
   i. Dial into our network using a virtual private network (VPN) when working from home
   ii. Enable multi-factor authentication where possible
   ii. Store passwords securely using a password manager

h. ICT Technical Support staff conduct regular access reviews to make sure each user in the Academy has the right level of permissions and admin rights

i. Have a firewall in place that is switched on

j. Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification

k. Monitor through the Business Continuity Plan the procedures for denial of access / loss of data or failure of technology.

# 18. A.I. APPLICATIONS

a. Artificial Intelligence (AI) is gaining greater use within education. City Learning Trust recognises that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff and reduce workload.The Trust also realises the risks involved in using AI systems, but that these may be mitigated through policies, procedures and guidelines

## 18.1 Acceptable Use of AI

a. I understand the Trust/Academy will monitor my use of AI applications when using trust equipment or login accounts.

b. I understand that I must treat AI applications as an outside entity and therefore all the rules and regulations of GDPR still apply.

a. I will not have conversations with AI that I would not have with a stranger – i.e. conversations including personal, medical, financial, or political subject matter about myself or about anyone else in the organisation.

b. I will not upload large amounts of personal data about our staff or students to an AI application i.e a spreadsheet full of names, national insurance numbers, and email addresses, efforts will be taken to anonymise this data before upload.d

d. I will only use the AI applications that have been approved in the list linked below, and if I wish to use another, I will contact the compliance officer to have my desired app reviewed and added to the approved list.

## 18.2 Approve AI App List

a. Microsoft Co-Pilot

b. Google Notebook LM

# 19. INTERNET ACCESS

a. The Academy's wireless internet connection is secure. We use filtering and separate connections for staff/ pupils/visitors (such as supply teachers).

## 19.1 Parents/Carers and Visitors

a. Parents/Carers and visitors to the Academy will not be permitted to use the Academy's WiFi unless specific authorisation is granted by the Headteacher/Principal or on specific Academy business.

b. The Headteacher/Principal will only grant authorisation if:
   i. Parents/Carers are working with the Academy in an official capacity (e.g. as a volunteer or as a member of the PTA)
   ii. Visitors need to access the Academy's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

c. Staff must not give WiFi password to anyone not authorised to have it. Doing so could result in disciplinary action.

# 20. CCTV

a. In order to regulate the management, operation, and use of the static closed-circuit television (CCTV) system at our Academies, we have outlined the specific purposes for which the CCTV system is used:
   i. To increase personal safety of pupils, staff and visitors, and reduce the risk of crime;
   ii. To protect the Academy buildings and their assets;
   iii. To assist in managing the Academy and ensure the security of the staff and children working on the site and visitors to the site;
   iv. To support the Police in a bid to deter and detect crime;
   v. To assist in identifying, apprehending and potentially prosecuting offenders.

## 20.1 Responsible People

a. The ICT Network Director holds overall responsibility for the CCTV on the Academy site.

## 20.2 Notification

a. The Academy Team will notify visitors to the site of the use of CCTV by the use of signs and when they sign in at the main reception. In addition to this, Parents/Carers will be informed through parent consent forms, as well as this policy suite, which will be available on the school website.

## 20.3 Security

a. Images filmed will be held in a secure location and can only be accessed by those who are authorised to do so.

b. The medium onto which we record images is: Hard drive / Cloud based drive.

c. It will be disposed of as follows: New recorded images overwrite the oldest stored images, typically after approximately 30 days though the period for which images are held may be shorter or longer than this.

## 20.4 Maintenance

a. A regular maintenance programme is in place and will be carried out by the IT Support Team during

b. Academy holidays or 3rd party service provider when required. Cameras will be checked every half term by the ICT Network Director and the IT Support Team.

## 20.5 Retention Period

a. Unless required for evidential purposes, the retention period of any images recorded by our CCTV footage is typically 6 weeks or less and any footage that is over this period will be destroyed in the following manner: Digital Images will be deleted by being overwritten.

## 20.6 Viewing

a. The locations that will be used for viewing of any images will be secure and only accessible by authorised personnel.

b. Authorisation to use the system must be obtained by request to the ICT Network Director.

c. Images will only be seen by 3rd parties if authorised by the Headteacher/Principal or their nominated Senior Leader. Should any images be required by the Police, we will follow this protocol:
   i. The request must be in written form, specifying the date and time (as far as possible) of the image;
   ii. The rank of the requesting officer must be Sergeant or above;
   iii. The school must provide a response to a request within 30 days;
   iv. If the decision is taken not to release the images, then the image in question must be held and not destroyed until all legal avenues have been exhausted.

## 20.7 Academy Closures

a. During times of Academy closure, the CCTV system will continue to operate as normal and will be maintained and monitored by the Site Manager and IT Support Team.

b. This information is published under the Freedom of Information Act and is available in hard copy by contacting the Academy Main Office.

# 21. DISPOSAL OF REDUNDANT ICT EQUIPMENT

a. All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

b. All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

c. Disposal of any ICT equipment will conform to:
   i. The Waste Electrical and Electronic Equipment Regulations 2006
   ii. The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
   iii. http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
   iv. http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
   v. http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
   vi. Data Protection Act 1998 (and General Data Protection Regulation 2018)
   vii. http://www.ico.gov.uk/what_we_cover/data_protection.aspx viii.Electricity at Work Regulations 1989
   viii.http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

d. The Trust maintains a comprehensive inventory of all its ICT equipment including a record of disposal this includes:
   i. Date item disposed of
   ii. Authorisation for disposal, including: verification of software licensing, Approval of the write-off of the equipment by the Finance Director
   iii. How it was disposed of e.g. waste, gift, sale
   iv. Name of person & / or organisation who received the disposed item
   v. Any redundant ICT equipment being considered for sale / gift will have been subject to a recent
   vi. electrical safety check and hold a valid PAT certificate.

## 22. DOCUMENT INFORMATION

| KEY INFORMATION | | |
|---|---|---|
| Policy Owner: | | ICT Network Director |
| Date Effective: | | January 2026 |
| Version: | | V2.2 |
| Frequency: | | Annual |
| Next Date: | | Spring Term 1 2027 |

| ASSOCIATED DOCUMENTS | |
|---|---|
| Safeguarding & Child Protection Policy<br>Behaviour | Code of Conduct<br>Data Protection<br>Complaints |

| DISTRIBUTION | |
|---|---|
| Name: | Academy Leads |
| Date: | 14.1.26 |
| Website/s: | n/r |

| REVIEW BODY | | |
|---|---|---|
| Name: | | Compliance Director |
| Date: | | 12.1.26 |

| APPROVAL | |
|---|---|
| Name: | Trustee Board |
| Date: | n/r |

**VERSION HISTORY**

| Version: | Date: | | Change: |
|---|---|---|---|
| 0.1 | January 2020 | New Document | New Policy |
| 1.0 | September 2020 | Format | Corporate format only |
| 1.1 | January 2021 | Interim update | Section 4.3 - Generic statement for named Trustee/ Governor |
| 1.2 | March 2022 | Annual review | Information Technology and Social Media policies referenced in Associated Documents and section 14.a |
| 1.3 | January 2023 | Interim review | References to online safety changed to e-safety. |
| 1.4 | January 2023 | Full review review | New fully revised Policy (Staff Version). |
| 1.5 | May 2023 | Interim update | Separate Student, Parents/Carers Version with Section 6, Appendix 1 and Appendix 6 removed. Under 'Link Policies', Staff Disciplinary and Code of Conduct references have also been removed from the student version. Otherwise, the versions are the same. |
| 1.6 | June 2023 | Proof reading typos | Minor typos/grammar corrected |
| 1.7 | February 2024 | Annual Review | Cross check all IT and Social Media aspects are covered and included. Full policy review |
| 2.0 | January 2025 | Annual review and re-write | Student and Staff versions merged. |
| 2.1 | March 2025 | Interim Update | Section 18 added for AI Use |
| 2.2 | January 2026 | Annual Review | Review and date changes only. |

# APPENDIX A

## Social Media Information for Staff

**Do not accept friend requests from pupils on social media**

### 10 rules for Academy staff on Social Media

a. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead

b. Change your profile picture to something unidentifiable, or if you don't, ensure that the image is professional

c. Check your privacy settings regularly

d. Be careful about tagging other staff members in images or posts

e. Don't share anything publicly that you wouldn't be just as happy showing your pupils

f. Don't use social media sites during Academy hours

g. Don't make comments about your job, your colleagues, our Academy or your pupils online – once it's out there, it's out there

h. Don't associate yourself with the Academy on your profile (e.g. by setting it as your workplace, or by 'checking in' at a Academy event)

i. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information

j. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as Parents/Carers or pupils)

### Check your privacy settings

a. Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

b. The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

c. **Google your name** to see what information about you is visible to the public

d. Prevent search engines from indexing your profile so that people can't search for you by name

e. Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

### What to do if …

#### A pupil adds you on social media

a. In the first instance, ignore and delete the request. Block the pupil from viewing your profile

b. Check your privacy settings again, and consider changing your display name or profile picture

c. If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify your Senior Leadership Team and/or their Parents/Carers. If the pupil persists, take a screenshot of their request and any accompanying messages, notify the Senior Leadership Team or the Headteacher/Principal about what's happening

#### A parent adds you on social media

a. It is at your discretion whether to respond, however, you would be advised not to accept. Bear in mind that:
   i. Responding to 1 parent's friend request or message might set an unwelcome precedent for both you and other teachers at the Academy
   ii. Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
   iii. If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

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

a. **Do not** retaliate or respond in any way
b. Save evidence of any abuse by taking screenshots and recording the time and date it occurred
c. Report the material to the relevant social network and ask them to remove it
d. If the perpetrator is a current pupil or staff member please speak to your Headteacher/Principal
e. If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
f. If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a Senior Leader should consider contacting the police

## Confidential Information

a. It is strictly forbidden to publish confidential information about, or in relation to, the CLT on Trust or personal social networking sites or blogs.
b. Confidential information includes unpublished details of current projects, financial information, school material, and student information. If you are in doubt as to whether the information is confidential or not, it should not be published.

## Protecting Privacy

a. Privacy settings on social networking sites that might allow others to post information, or see information that is private or personal, should be set to limit access to trusted parties only. At all times, employees must be mindful of posting information that you would not want the general public to see.
b. What you publish may be around for a long time, so consider the content carefully and be especially cautious about disclosing personal details in your posts and blogs.

## Copyright

a. You should never quote more than short excerpts of someone else's work, and always attribute such work to the original author/source. It is good general practice to link to others' work rather than reproduce it.

## Honesty, Transparency And Integrity

a. Do not say anything that is dishonest, untrue, or misleading. If you have a vested interest in something you are discussing, point it out.
b. If you make an error, be up front about your mistake and correct it quickly. If you choose to modify an earlier post, make it clear that you have done so.

## Respecting Your Audience

a. The public in general, and CLT employees and students, reflect a diverse set of customs, values and points of view. Don't be afraid to be yourself, but do so respectfully. This includes not only the obvious (i.e. no ethnic slurs, offensive or defamatory comments, personal insults or obscenities), but also proper consideration of privacy and of topics that may be considered objectionable or inflammatory - such as politics and religion.
b. Use your best judgement and be sure to make it clear that the views and opinions expressed are yours alone and do not represent the official views of CLT.

## Protecting Our Partners

a. Partner schools or students should not be cited, or obviously referenced without their prior approval.
b. Never identify a partner or student by name without permission and never discuss confidential details of partner/ supplier engagement.
c. Staff must not befriend students who are currently at the school or the City College and should exercise common sense and mature judgements when befriending ex-students, considering the age, maturity and behaviour whilst they were attending the Academy. Staff should consider if the ex- student has siblings currently at the Academy or 6th form and should not befriend if this is the case.

## Misrepresentation And Disclaimers

a. If you see misrepresentations made about CLT you should make your line manager aware at earliest opportunity.
b. If you speak about others, make sure what you say is factual and that you do not resort to criticism of that party.
c. Avoid online arguments. Don't try to settle scores or goad fellow bloggers, competitors or others into inflammatory debates.
d. Many social media users include a prominent disclaimer saying who they work for, but that anything that they publish is their personal opinion, and not necessarily the opinion of the company they work for (i.e. CLT).

## Use At Work

a. Social networking, including blogging, must not interfere with your responsibilities and tasks during working hours.

b. It is permitted to use social networking sites only in designated break and lunch times, and in accordance with this procedure

## Disciplinary Action

a. Using your blog or social media micro-site to publicly criticise, spread false rumours about the CLT, our partners, or your co-workers may lead to disciplinary and/or legal action.

b. Violation of the use at work section of this procedure may result in disciplinary action, up to and including termination of an employee's contract of employment.

## APPENDIX B

### Acceptable use of the internet: Agreement for Parents/Carers

| Acceptable use of the internet: Agreement for Parents/Carers | |
|---|---|
| **Name of parent/carer:**<br><br>**Name of child:** | |
| Online channels are an important way for parents/carers to communicate with, or about, our Academy. The Academy uses the following channels:<br>- Our official website<br>- Our official Social Media Channels<br>- Our virtual learning platforms<br>- Our online parent booking systems<br>- Email/ texts to parents/carers for Academy announcements and information | |
| When communicating with the Academy via official communication channels, or using private/ independent channels to talk about the Academy, I will:<br>• Be respectful towards members of staff, and the Academy, at all times<br>• Be respectful of other parents/carers and children<br>• Direct any complaints or concerns through the Academy's official channels, so they can be dealt with in line with the Academy's complaints procedure<br>I will not:<br>• Use private groups, the Academy's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the Academy cannot improve or address issues unless they are raised in an appropriate way<br>• Use private groups, the Academy's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the Academy and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident.<br>• Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other child's parents/carers. | |
| **Signed:** | **Date:** |

# APPENDIX C

## Acceptable Use Agreement for Pupils

| **Acceptable use of the Academy's ICT facilities and internet: Agreement for pupils** | |
|---|---|
| **Name of pupil:** | |
| **When using the Academy's ICT facilities and accessing the internet in the Academy, I will not:**<br>• Use the facilities or internet for a non-educational purpose<br>• Use the facilities without a teacher being present, or without a teacher's permission<br>• Use the facilities to break Academy rules<br>• Access any inappropriate websites<br>• Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)<br>• Use chat rooms<br>• Open any attachments in emails, or follow any links in emails, without first checking with a teacher<br>• Use any inappropriate language when communicating online, including in emails<br>• Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video<br>• Share my password with others or log in to the Academy's network using someone else's details<br>• Bully other people<br>• Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer<br>• Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision<br>• I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.<br>• I will always use the Academy's ICT systems and internet responsibly.<br>If I bring a personal mobile phone or other personal electronic device into the Academy:<br>• I will only use it for learning purposes and I will allow any monitoring and device management software to be added to my device (such as SENSO-Cloud) before using the device on site<br>• I will not use it during lessons, tutor group time, clubs or other activities organised by the Academy, without a teacher's permission<br>• I will use it responsibly, outside the Academy building and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online<br>• I agree that the Academy will monitor the websites I visit if using a personal device or an Academy provided one and the ICT facilities and systems I access.<br>I understand that the Academy can discipline me if I do certain unacceptable things online, even if I'm not in the Academy when I do them. | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer agreement:** I agree that my child can use the Academy's ICT systems and internet when appropriately supervised by a member of Academy staff. I agree to the conditions set out above for pupils using the Academy's ICT systems and internet, and for using personal electronic devices in Academy, and will make sure my child understands these. | |
| **Signed (parent/carer):** | **Date:** |

# APPENDIX D

## Acceptable use agreement for staff, governors, volunteers and visitors

| Acceptable use of the Academy's ICT facilities and the internet: Agreement for staff, governors, volunteers and visitors | |
|---|---|
| **Name of staff member/governor/volunteer/visitor:** | |
| When using the Academy's ICT facilities and accessing the internet in the Academy, or outside the Academy on a work device, I will not:<br>• Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)<br>• Use them in any way which could harm the Academy's reputation<br>• Use any improper language when communicating online, including in emails or other messaging services<br>• Install any unauthorised software, or connect unauthorised hardware or devices to the Academy's network<br>• Share my password with others or log-in to the Academy's network using someone else's details<br>• Share confidential information about the Academy, its pupils or staff, or other members of the community<br>• Access, modify or share data I'm not authorised to access, modify or share<br>• Promote private businesses, unless that business is directly related to the Academy | |
| I understand that the Academy will monitor the websites I visit and my use of the Academy's ICT facilities and systems.<br><br>I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the Academy, and keep all data securely stored in accordance with this policy and the Academy's data protection policy.<br><br>I will let the Designated Safeguarding Lead (DSL) and ICT Network Director know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.<br>I will always use the Academy's ICT systems and internet responsibly, and ensure that pupils in my care do so too.<br>If I am using my own device for work related purposes, I agree that monitoring management systems will be downloaded and monitored as if they were an Academy device, for the safeguarding and protection of children. I will make the ICT Network Director aware of any personal equipment and devices I bring into the Academy before being used for educational purposes.<br><br>If using my personal mobile phone on site, this will be out of view of students and during non-contact time, in accordance with the Code of Conduct. | |
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

# APPENDIX E

## Glossary of Cyber Security Terminology

These key terms will help you to understand the common forms of cyber attack and the measures the Academy will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

| TERM | DEFINITION |
|---|---|
| **Antivirus** | Software designed to detect, stop and remove malicious software and viruses. |
| **Breach** | When your data, systems or networks are accessed or changed in a non-authorised way. |
| **Cloud** | Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices. |
| **Cyber attack** | An attempt to access, damage or disrupt your computer systems, networks or devices maliciously. |
| **Cyber incident** | Where the security of your system or service has been breached. |
| **Cyber security** | The protection of your devices, services and networks (and the information they contain) from theft or damage. |
| **Download attack** | Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent. |
| **Firewall** | Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network. |
| **Hacker** | Someone with some computer skills who uses them to break into computers, systems and networks. |
| **Malware** | Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations. |
| **Patching** | Updating firmware or software to improve security and/ or enhance functionality. |
| **Pentest** | Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses. |
| **Pharming** | An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address. |
| **Phishing** | Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website. |
| **Ransomware** | Malicious software that stops you from using your data or systems until you make a payment. |
| **Social engineering** | Manipulating people into giving information or carrying out specific actions that an attacker can use. |
| **Spear-phishing** | A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts. |
| **Trojan** | A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer. |
| **Two-factor/multi-factor authentication** | Using 2 or more different components to verify a user's identity. |
| **Virus** | Programmes designed to self-replicate and infect legitimate software programmes or systems. |
| **Virtual private network (VPN)** | An encrypted network which allows remote users to connect securely. |
| **Whaling** | Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation. |

# APPENDIX F

## Laptop and Device Loan Agreement for Staff

This document outlines an agreement between the City Learning Trust (as the provider of the device) and the recipient of the device.

| | |
|---|---|
| Recipient | |
| Item Description | |
| Serial Number | |

The laptop/device is issued to you for the following purposes:

- To access your email on a daily basis
- To complete online registration and reports
- To support teaching and learning, including the use of the VLE

You will be responsible for the security of the confidential information which can be accessed by or stored on your device. All sources of such data should be protected by a secure password (minimum of 8 characters including at least one letter and one number) and must be protected from the sight of students or the possibility of unauthorised access (see Data Protection Policy for more information).

The school's insurance policy covers the laptop/device against theft whilst it is in school, provided that it is not left unattended.

Please read the following agreement carefully before signing:

I understand that the laptop/device is being loaned to me for use in school and at home according to the acceptable use policy laid out by the Trust (attached). I understand the laptop remains the property of The City Learning Trust at all times and that it is to be returned in good condition when I (the recipient) leaves employment or on completion of my contract with the Trust.

I understand that I must return the laptop/device when requested for maintenance work and that I must not install any programmes without the approval of the ICT Network Director. I undertake not to store any materials on the machine which would infringe the copyright of such materials. Extended absence of more than three weeks may require the member of staff to return their laptop to support teaching and learning.

Monitoring and remote support tools are installed on the device to provide safeguarding measures and to facilitate remote technical support. This software will be used for this purpose only, except in the case of any legal investigations.

I will be responsible for the care and safety of the device and will take all reasonable precautions to ensure that it does not become damaged or lost. I understand that I will be liable for the cost of replacing or repairing a machine which has been lost, stolen or damaged as a result of negligence on my part.

IF THE EQUIPMENT IS LOST OR DAMAGED, YOU MUST INFORM THE ICT NETWORK DIRECTOR IMMEDIATELY.

**Signature ..... Date ..... Full Name (printed)**

| | |
|---|---|
| Returned Date | |

# APPENDIX G

## Laptop and Device Loan Agreement for Pupils

This document outlines an agreement between the City Learning Trust (as the provider of the device) and the recipient of the device (the pupil).

| | |
|---|---|
| Pupil Name | |
| Item Description | |
| Serial Number | |

The laptop/device is issued to you for the following purposes:

- To access your school email
- To complete online work, access the internet for school purposes and access any online learning
- To support teaching and learning, including the use of the VLE or other teaching platforms

You will be responsible for the security of the confidential information which can be accessed by or stored on your device. Your device should be protected by a secure password (minimum of 8 characters including at least one letter and one number) and must be protected from the sight of others or the possibility of unauthorised access.

The school's insurance policy covers the laptop/device against theft whilst it is in school, provided that it is not left unattended.

Please read the following agreement carefully before signing:

I understand that the laptop/device is being loaned to me for use in school and at home according to the acceptable use policy laid out by the Trust (attached). I understand the laptop remains the property of The City Learning Trust at all times and that it is to be returned in good condition when I (the recipient/pupil) leaves the school.

I understand that I must return the laptop/device when requested for maintenance work and that I must not install any programmes without the approval of the ICT Network Director. I undertake not to store any materials on the machine which would infringe the copyright of such materials. I can be asked to give the laptop/device back if I do not use it responsibly.

Monitoring and remote support tools are installed on the device to provide safeguarding measures and to facilitate remote technical support. This software will be used for this purpose only, except in the case of any legal investigations.

I will be responsible for the care and safety of the device and will take all reasonable precautions to ensure that it does not become damaged or lost. I understand that my parents/carers may be liable for the cost of replacing or repairing a machine which has been lost, stolen or damaged as a result of negligence on my part.

IF THE EQUIPMENT IS LOST OR DAMAGED, YOU MUST INFORM THE ICT NETWORK DIRECTOR IMMEDIATELY.

Signature ..... Date ..... Full Name (printed)

| | |
|---|---|
| Returned Date | |