

E-SAFETY AND INFORMATION COMMUNICATIONS TECHNOLOGY POLICY

Document Owner: ICT Network Director

Date: March 2023

Status: Non-statutory



City Learning Trust

Inspiring Outstanding Achievement

Document Type	E-Safety and Information Communications Technology Policy			
Reference/Version Number	CLT-ESP-V1.6/Stu			
Summary	This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for Academies on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.			
Associated Documents	Child Protection and Safeguarding policy Behaviour Policy Social Media Policy IT Policy	Staff Disciplinary Procedures Data Protection Policy and Privacy Notices Complaints Procedure		
Target Audience	Students and Parent/Carers			
Date of this Version	March 2023			
Document Owner	ICT Network Director			
Review Body	Policy Admin Group	Meeting Date	15.6.22 11.5.23	
Union Consultation Date/s:	N/A	Meeting Date	N/A	
Proof Read	K Smith - 24.4.23			
Senior Leadership Team	N/A			
Approved/Ratified by	Board of Trustees	Meeting Date	17.12.18 14.12.20 18.7.22	
Review Frequency	Annual	Next Review Date	1.2.24	
Date uploaded on website/s				
CLT n/r	Haywood n/r	Trentham n/r	Mill Hill n/r	Smallthorne n/r
Date uploaded to Sharepoint/s				
CLT V1.2 - 15.6.22	Haywood V1.1 11.12.20 15:14 V1.2 - 15.6.22	Trentham V1.1 11.12.20 15:14 V1.2 - 15.6.22	Mill Hill V1.1 11.12.20 15:14 V1.2 - 15.6.22	Smallthorne V1.1 11.12.20 15:14 V1.2 - 15.6.22
Acknowledged by Local Governing Committee/s:				
Acknowledged by Local Governing Committee/s:	Haywood 3.4.19 1.12.20 5.7.22	Trentham 21.3.19 2.12.19 6.7.22	Mill Hill 20.3.19 18.11.20 29.3.22	Smallthorne 26.3.19 18.11.20 29.3.22

VERSION CONTROL

Version No:	Type of change	Date	Revisions from previous version
0.1	New Document	Jan 2020	New Policy
1.0	Format	Sept 2020	Corporate format only, no other changes
1.1	Section 4.3	Jan 2021	Generic statement for named Trustee/Governor
1.2	Annual Review	Mar 2022	Information Technology and Social Media policies referenced in Associated Documents and section 14.a
1.3	Interim review from PPWG	Jan 2023	All references to online safety changed to e-safety.
1.4	Full review and re-draft	Mar 2023	New fully revised Policy
1.5	Further update	May 2023	Students, Parent/Carers Version has Section 6, Appendix 1 and Appendix 6 removed. Under 'Link Policies', Staff Disciplinary and Code of Conduct references have ualso been removed from the student version. Otherwise, the versions are the same.
1.6	Proof reading typos	June 2023	Minor typos/grammar corrected

TABLE OF CONTENTS

VERSION CONTROL	2
TABLE OF CONTENTS	3
1. INTRODUCTION AND AIMS	5
2. RELEVANT LEGISLATION AND GUIDANCE	5
3. DEFINITIONS	6
3.1 ICT Facilities	6
3.2 Users	6
3.3 Personal Use	6
3.4 Authorised Personnel	6
3.5 Materials	6
4. ROLES AND RESPONSIBILITIES	6
4.1 The Local Governing Committee	6
4.2 The Headteacher/Principal	6
4.3 The Designated Safeguarding Lead	6
4.4 The ICT Network Director	7
4.5 All Staff and Volunteers	7
4.6 Parents/Carers	7
4.7 Visitors and Members of the Community	7
5. UNACCEPTABLE USE	8
5.1 Exceptions From Unacceptable Use	8
5.2 Sanctions	8
6. STAFF (Including Governors, Volunteers, and Contractors)	9
7. MONITORING AND ACCESS	9
8. DATA PROTECTION AND UYOD	9
9. REMOTE ACCESS	9
10. ACADEMY SOCIAL MEDIA ACCOUNTS	9
11. MONITORING AND FILTERING OF THE ACADEMY NETWORK AND USE OF ICT FACILITIES	9
12. PUPILS	10
12.1 Access to ICT Facilities	10
12.2 Acceptable Use Agreement: Students	10
12.3 Search and Deletion	11
12.4 Unacceptable Use of ICT and the Internet Outside of Academy	12
13. E-SAFETY EDUCATION	13
14. CYBER BULLYING	13
14.1 Definition	13
14.2 Preventing and Addressing Cyber-Bullying	13
15. REMOTE LEARNING (Pupils)	13
15.1 Pupils	13
15.2 Parents/Carers	14
15.2.1 Access to ICT Facilities and Materials	14
15.2.2 Communicating with or about the Academy Online	14
15.2.3 Communicating with Parents/Carers about Pupil Activity	14
16. DATA SECURITY	14
16.1 Passwords and Password Security	14

16.2 Passwords	15
16.3 Password Security	15
16.4 Software Updates, Firewalls and Anti-Virus Software	15
16.5 Data Protection	15
16.6 Access to Facilities and Materials	15
16.7 Encryption	16
17.PROTECTION FROM CYBER ATTACKS	16
18.INTERNET ACCESS	16
18.1 Parents/Carers and Visitors	16
19.CCTV	17
19.1 Responsible People	17
19.2 Notification	17
19.3 Security	17
19.4 Maintenance	17
19.5 Retention Period	17
19.6 Viewing	17
19.7 Academy Closures	17
20.DISPOSAL OF REDUNDANT ICT EQUIPMENT	18
21.MONITORING AND REVIEW	18
22.RELATED POLICIES	18
APPENDIX A	19
APPENDIX B	20
Acceptable use of the internet: Agreement for Parents/Carers	20
APPENDIX C	21
Acceptable Use Agreement for Pupils	21
APPENDIX D	22
Acceptable use agreement for visitors	22
APPENDIX E	23
Glossary of Cyber Security Terminology	23
APPENDIX F	25
Laptop and Device Loan Agreement for Staff	25
APPENDIX G	26
Laptop and Device Loan Agreement for Pupils	26

1. INTRODUCTION AND AIMS

- 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 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 2022](#)
 - x. [Searching, screening and confiscation: advice for Academics 2022](#)
 - xi. [National Cyber Security Centre \(NCSC\): Cyber Security for Academics](#)
 - 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 Academics 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 which 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. ROLES AND RESPONSIBILITIES

4.1 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 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

4.2 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.

4.3 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 that any incidents of cyber-bullying are logged and dealt with appropriately in line with the 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.

4.4 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 that any online safety incidents are logged on CPOMS (or relevant recording procedures) and dealt with appropriately in line with this policy
 - vi. Ensuring that 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.

4.5 All 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:** The Social Media policy works alongside the E-Safety and Information Communications Technology Policy, and should therefore be read in conjunction.
 - ii. Implementing this policy consistently
 - iii. Agreeing and adhering to the terms on acceptable use of the Academy's ICT systems and the internet, and ensuring that pupils follow the Academy's terms on acceptable use
 - iv. Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
 - v. 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.

4.6 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 the terms on acceptable use of the Academy's ICT systems and internet
- b. Parents/Carers can seek further guidance on keeping children safe online from the following organisations and websites:
 - i. What are the 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. Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

4.7 Visitors and Members of the Community

- a. 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.

5. 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
- b. 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.

5.1 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.

5.2 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.

6. STAFF (Including Governors, Volunteers, and Contractors)

This section is for Staff only guidance and as this is not required in the Students/Parents and Carers version of this policy, it has been removed.

Please contact the Academy Office if you require any information regarding this section of the policy.

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

This section is for Staff only guidance and as this is not required in the Students/Parents and Carers version of this policy, it has been removed.

Please contact the Academy Office if you require any information regarding this section of the policy.

10. ACADEMY SOCIAL MEDIA ACCOUNTS

This section is for Staff only guidance and as this is not required in the Students/Parents and Carers version of this policy, it has been removed.

Please contact the Academy Office if you require any information regarding this section of the policy.

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. Bandwidth usage
 - iii. Email accounts
 - iv. Telephone calls
 - v. User activity/access logs
 - vi. Any other electronic communications

- b. 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.
- c. Where appropriate, authorised personnel may raise concerns about monitored activity with the Academy's designated safeguarding lead (DSL) and ICT Network Director as appropriate.
- d. 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.
- e. 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:
 - i. 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.
 - ii. 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 the 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 (Pupils)

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 Academics 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 the Academy's ICT facilities should set strong passwords for their accounts and keep these 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 logon. Do not include passwords in any automated logon procedures
- c. Staff and Students should change temporary passwords at first logon
- 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 within 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.
- 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 login details
 - Verify requests for payments or changes to information
 - iii. Make sure staff are aware of our procedures for reporting and responding to cyber security incidents
 - iv. Investigate whether our IT software needs updating or replacing to be more secure
 - v. Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
 - vi. Put controls in place that are:
 - **Proportionate:** the Academy will verify this annually, using a third-party audit, to objectively test that what it has in place is effective
 - **Multi-layered:** everyone will be clear on what to look out for to keep our systems safe
 - **Up to date:** with a system in place to monitor when the Academy needs to update its software
 - **Regularly reviewed and tested:** to make sure the systems are as effective and secure as they can be
 - Back up critical data daily and store these backups on cloud based backup systems.
 - vii. Make sure staff:
 - Dial into our network using a virtual private network (VPN) when working from home
 - Enable multi-factor authentication where possible
 - Store passwords securely using a password manager
 - viii. 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
 - ix. Have a firewall in place that is switched on
 - x. 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
 - xi. Monitor through the Business Continuity Plan the procedures for denial of access / loss of data or failure of technology.

18. 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).

18.1 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 the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

19. CCTV

- a. In order to regulate the management, operation and use of the static system, closed circuit television (CCTV) system at our Academy, the purposes for which the CCTV Systems are used are:
 - 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.

19.1 Responsible People

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

19.2 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.

19.3 Security

- a. a. The images that are 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.

19.4 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.

19.5 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.

19.6 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.

19.7 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.

20. 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
 - ix. 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.

21. MONITORING AND REVIEW

- a. The Headteacher/Principal and ICT Network Director, monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Academy. This policy will be reviewed annually by the Local Governing Committee and PPWG.

22. RELATED POLICIES

- a. This policy should be read alongside the Academy's policies on:
 - i. Social Media
 - ii. Safeguarding and Child Protection
 - iii. Behaviour
 - iv. Code of Conduct
 - v. Data Protection
 - vi. IT Policy
 - vii. Using Your Own Device Policy

APPENDIX A

This section is for Staff only guidance and as this is not required in the Students/Parents and Carers version of this policy, it has been removed.

Please contact the Academy Office if you require any information regarding this section of the policy.

APPENDIX B

Acceptable use of the internet: Agreement for Parents/Carers

Acceptable use of the internet: Agreement for Parents/Carers

Name of parent/carers:

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:

- Our official website
- Our official Social Media Channels
- Our virtual learning platforms
- Our online parent booking systems
- 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:

- Be respectful towards members of staff, and the Academy, at all times
- Be respectful of other parents/carers and children
- 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

I will not:

- 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
- 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.
- 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:

- Use the facilities or internet for a non-educational purpose
- Use the facilities without a teacher being present, or without a teacher's permission
- Use the facilities to break Academy rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- 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
- Share my password with others or log in to the Academy's network using someone else's details
- Bully other people
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- 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.
- I will always use the Academy's ICT systems and internet responsibly.

If I bring a personal mobile phone or other personal electronic device into the Academy:

- 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
- I will not use it during lessons, tutor group time, clubs or other activities organised by the Academy, without a teacher's permission
- 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
- 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.

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 visitors

Acceptable use of the Academy's ICT facilities and the internet: Agreement for visitors

Name of 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:

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

I understand that the Academy will monitor the websites I visit and my use of the Academy's ICT facilities and systems.

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.

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.

I will always use the Academy's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

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.

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 (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.

TERM	DEFINITION
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	
---------------	--