E-SAFETY POLICY

A policy for the acceptable use of Trust ICT Equipment

PHASE	**SECONDARY & JUNIOR**
POLICY LEAD	**MATTHEW SUTTON** **(ACET Network Manager)**
DATE OF APPROVAL BY TRUSTEES	**25th JULY 2022**
DATE OF RECEIPT BY LOCAL GOVERNING BODY	**OCTOBER 2022**
FREQUENCY DATE	**ANNUALLY**
NEXT REVIEW DATE	**JUNE 2023**

Contents

1. Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, academies need to build-in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Social Networking, Instant Messaging and forums
- Mobile/ Smart devices with text, video and web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting, Video Broadcasting
- Music Downloading / Streaming

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements.

At ACET, we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Academies hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, sanctions in the way of fines and potentially damage the reputation of an academy or the Trust. This can make it more difficult for our academy to use technology to benefit learners.

Everybody in the Trust has a shared responsibility to ensure the safety of our pupils / students and the security of any sensitive information used in their day to day professional duties; even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils / students) are inclusive of both fixed and mobile Internet; technologies provided by the Trust (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto academy premises (BYOD – see section 10.0 of this document)

The purpose of these documents is to ensure Trust-wide compliance with procedures and guidelines concerning all ICT equipment (networked or otherwise), telecommunications activities, data storage, use of network-attached devices, and any other associated software or hardware. This document covers such areas as:

- IT Network access;
- Data usage and security– either by storing, transmitting and receiving;
- Internet and intranet access and usage;
- Email usage;
- Access to other equipment;
- The use of mobile devices;
- The use of Social Media such as blogs, wiki, message boards and social websites (such as Facebook);
- Using your own equipment (BYOD);
- Monitoring the use of equipment;
- How breaches of these policies are handled;
- Accessing cloud based technologies;
- Disposing of redundant equipment;
- Parental involvement;
- Current Legislation governing Data Protection, Privacy, Human Rights, Copyright and other relevant Acts

The documents aims to ensure all staff, pupils / students, Governors and third parties are aware of the measures taken to ensure the security and integrity of the Trust IT Network Facility, the equipment used and the data it holds. It also defines the responsibility for all users and the consequences appropriate to the misuse of equipment, data and other information.

2. GDPR

The General Data Protection Regulation (GDPR) 2018 is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. GDPR replaced the data protection directive of 1998 and became enforceable from 25 May 2018. Unlike a directive, it does not require national governments to pass any enabling legislation, and is thus directly binding and applicable.

A full guide the General Data Protection Regulations is available from the gov.uk website:

https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

2.1 GDPR and Brexit

The Brexit transition period ended on 31st December 2020. The UK's Data Protect Act 2018 has already enacted the EU GDPR's requirements into UK law, and with effect from 1 January 2021, the DPPEC (Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit)) Regulations 2019 amended the DPA 2018 and merged it with the requirements of the EU GDPR to form a new, UK specific data protection regime that works in a UK context after Brexit as part of the DPA 2018.

This new regime is known as 'the UK GDPR'.

This document covers the acceptable use of Trust IT equipment as well as the electronic use of data and the devices that are used to store, retrieve, distribute and manipulate data as it relates to the ACET privacy notices.

The ACET GDPR policy is a comprehensive document intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. The full document plus the ACET Privacy notices for Staff and pupils / students can be downloaded from the ACET website: www.astoncetrust.org

3. Document Revision

Date	Version	Revision	Revised By
20th October 2014	1.00	Initial DRAFT – **Not for general distribution.**	D. Armstrong
11th November 2014	1.10	Updated Draft – Distribution to D. Richardson and D. Taylor Only. **NOT FOR GENERAL DISTRIBUTION**	D. Armstrong
10th March 2015	1.20	Amended text to instruct users on access for email and the VLE. This document is still unapproved and **NOT FOR GENERAL DISTRIBUTION**	D. Armstrong
5th June 2015	1.21	Change the location of access to email from https://portal.aston.rotherham.sch.uk to https://access.astoncetrust.org **– NOT FOR DISTRIBUTION**	D. Armstrong
10th June 2015	1.22	Updated section on Social Media. **NON RATIFIED Version and NOT FOR DISTRIBUTION.**	D. Armstrong
February 2016	1.23	Approved	D. Armstrong
June 2016	1.24	Updates to 3.1 Data Security. This includes updates to the Privacy Shield / Safe Harbor information from the ICO	D. Armstrong
January 2018	1.25	GDPR Introduction	D. Armstrong
January 2019	1.26	ACET privacy policy references. GDPR replaces Data Protection Act Updates to some sentences that clarify previously stated policies. Added a number of items in the glossary Further updates to 3.1 Data Security relating to Privacy Shield	D Armstrong

June 2020	1.27	Removed references to this policy where it also included the words 'Data Protection' Added 'Streaming' to the uses of Internet connectivity Update section 1.2 to indicate where the GDPR policy and Privacy notices can be downloaded Added a number of lines relating to GDPR in sections 3.0 and 6.2 Added a line regarding the ownership of email mailboxes and files in section 3.2 Section 4 has been updated to include a note about the risks of using unencrypted portable media. Updated section 4.1 to clarify that the prohibition on the installation of software does not extend to device drivers (for personal printers for example) Explained the use of the Internet when connected to the Trust VPN (section 5.1) Changed the address that staff can access email in section 6.0 Removed the reference to Two Factor Authentication from section 6.0 Added section for Cloud based services Updated some lines to bold text to add emphasis Removed references to social networks that no longer exist Updated the glossary with additional terms	D. Armstrong

June 2021	1.28	Section 2.1 GDPR and effect on this policy following the Brexit transition period. Adjusted all references to GDPR to read 'UK GDPR' Remove items related to the storage of data outside of the EU and EEA that do not apply to the UK, including changes to Privacy Shield. References added. Added section 4.2 and section 19 to outline the process of an IT investigation into security breaches or IT related safeguarding concerns. Updated various links to legislation where that is different from the previous version of this policy. Adjusted section 8.2 inserting information on the risks of sending email unencrypted or by sending a password to a protected document in the same email or to the same email address. Changed references to 'Students' to 'Pupils / Students' throughout the document. Added a note about data backups and the Google Gmail System in section 9.1 Added notes on the use of third party VPN software on Trust equipment in section 10. Added additional information in section 11.2 regarding the general guidance for the general use of social media and Teacher Standards. Added links in section 11.4 to the help and privacy sections of the most popular social media and messaging sites. Added new, removed irrelevant, and updated existing notes on legislation in section 15.	
June 2022	1.29	Section 8 modified to reflect use of Office 365 as the email platform rather than on-premise Exchange Section 12 edited to reflect use of Office 365 as the email platform and removed outdated advice on how to access emails.	M Sutton

4. Security & Privacy

Security on any computer system is a high priority, especially when it involves many users and sensitive data. The Trust has implemented a number of security measures to protect your access to the network and the data stored on it. **It is imperative that should you discover or have identified a security issue with the network you inform The Trust IT Services Manager or other IT Technical Support Technician immediately**. Do not demonstrate any issue to other users, do not attempt to correct the issue yourself or seek to exploit it. The ACET Privacy notices for Staff and Pupils / students can be downloaded from the ACET website:

www.astoncetrust.org

The accessing, storage and appropriate use of data is something the Trust takes very seriously. Data is held on a central computer network and distributed across multiple academies, categorised and secured to prevent unauthorised access. Your own data (that is your documents, images and any music or video files) are only accessible by logging onto the computer network with your username and password (or those of the system administrator for the explicit purpose of securing and auditing that data). Personnel data which is data that relates to an individual and can be used to identify them, or be attributed to them is secured in our Management Information System (MIS) database and in various document stores on the Trust file storage systems. Access to the Student records area of this system is generally given to teaching staff with some support staff having additional access to personnel information. Such information is held, stored and processed in accordance with the ACET privacy notices and with references to the Information Commissioner's Office documents:

http://ico.org.uk/for_organisations/data_protection/security_measures
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

It is the responsibility of all staff to ensure personal, sensitive and confidential information is protected (ref. GDPR Policy). Any data stored on any portable media could be read in any computer by anyone not associated with the Trust unless it is encrypted or secured with a password. Storing data on unencrypted media poses a risk of a data breach if that media is lost or stolen. If any data of the following nature is to be stored on any portable device (memory stick or hard drive) and you wish to encrypt your device, or password protect the documents it contains, then please contact IT Support who will be happy to help.

- Can be used to identify any member of staff or student;
- contains personal information that is not meant for the public domain;
- contains business related information from any academy (including financial data, business practices and policies or other confidential information)

In addition, and as the Trust has no control over what happens to data once it leaves the Trust IT network or premises, storing that information on cloud based storage servers should not be considered secure, based on the UK data protection principles. The European Data Protection Board (EDPB) and other countries developed the GDPR (2018) policy to enable the safe use of these services, however, since end of the Brexit transition (31st Dec 2020) the UK has not adopted an adequacy decision for the United States or for the EU-US Privacy Shield Framework.

https://www.privacyshield.gov/article?id=Privacy-Shield-and-the-UK-FAQs

- Is encrypted at source and stored in that manner until retrieved or removed.
- Is encrypted at destination and remains so until removed.

If you require access to these services within school, please contact the IT Support department with your request, stating the need for that access and the type of data you wish to store or retrieve.

Unless authorised to do so, members of staff should not copy, transmit, print or scan any confidential personal information to any person or persons either internally or externally who does not have a need to know that information. In addition you should not attempt to access, receive or solicit personal data or information if you do not need to know that information.

You should also ensure that any data transmitted or passed to third parties conforms to the Trust privacy policy and any privacy policy issued by that third party. If any doubt exists, advice from the IT Services Manager should be sought before any data is released to anyone outside of the Trust academies.

Please ensure your usernames and passwords are kept secure and do not divulged them to anyone.

If you have any further queries regarding access to any of these services, please contact a member of the IT Support team who will help you with your query.

4.1 Privacy and Monitoring at Work

Workplace Monitoring and the monitoring of electronic communications at work are covered by UK & EU data protection and privacy laws. These laws do not prevent the monitoring of electronic communications or other workplace monitoring however, they do limit what can be monitored and when this information can be collected, stored and analysed. Forms of monitoring can include (but is not limited to):

- Recording via CCTV cameras;
- Accessing, and reviewing email communications;
- Checking telephone logs or recording phone calls (including mobile phones);
- Collecting information regarding website access or Internet usage

It should be noted that it cannot be guaranteed that where the private use of Trust or academy owned equipment is permitted, any personal information you store, or communications you have made will not be discovered either during any inspection or by maintenance procedures. IT Support cannot be responsible if personal data is lost during any inspection, monitoring or maintenance process.

There are several Laws, Regulations, Codes of Practice and general guidance documents for academies to refer to when considering monitoring. These include the ICO Monitoring at Work codes of Practice (Employment Practices Code – 2011) Part 3 (section 3.2 - all parts and 3.4 – all parts), the UK General Data Protection Regulation (UK GDPR) – Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. A full list of the legislation covering IT related issues and used by this policy are listed in section 12. In addition, IT Technical staff (under the direct request of the Chief Executive Officer (CEO) or Trust Director) may monitor, intercept, access, inspect, record or disclose any or all information or communication of personnel who are absent from the workplace for any reasonable length of time. The ownership of the mailboxes and files of individual members of staff remains with them and permission will be sought where information contained therein is requested to be shared with third parties

It is important to understand that your use of the Trust IT Systems, the data you hold and your Internet and email activity may be monitored by the Chief Executive Officer (CEO) (or the Trust IT Services Manager under the request of the Chief Executive Officer). Monitoring of this kind is not a routine act and will only be entered into under the particular circumstances, some of which may be:

- Where the monitoring relates to the business of the Trust;
- Where monitoring is used to enhance, review or confirm the appropriateness of policies or procedures;
- To prevent or detect crime;
- To enforce the protection of the staff and pupils / students in any of our Academies;
- If there are reasonable grounds to suspect sustained or repeated breaches of this or other policies;

- A safeguarding issue is reported;
- Where there is a requirement to obtain information requested by a law enforcement authority for child protection issues or the safety of staff;

You can find further information regarding monitoring at work and the monitoring of electronic communications from the following websites:

https://www.gov.uk/monitoring-work-workers-rights/overview

http://www.adviceguide.org.uk/england/work_e/work_rights_at_work_e/monitoring_at_work.htm

https://www.citizensadvice.org.uk/work/rights-at-work/basic-rights-and-contracts/monitoring-at-work/

In most cases you will be informed that this monitoring is taking place and for what purpose.

4.2 Investigation into IT security breach or IT safeguarding issue

IT Support will carry out any investigations into breaches of security, this policy or, in the case of pupils/students where a breach of the Acceptable Use of Equipment or where a safeguarding concern regarding the use of IT equipment is raised. Any investigation is based on a policy as laid out in the 'Request for IT Investigation' online form and procedure. This form will be completed by the IT department in all investigations and will form the basis of any investigation. This procedure is only carried out under instruction from the Principal of the academy and follows the guidelines set out in section 4 (all parts) of this policy. The form and procedure is stored on line as a google form. A version of this is available to view in section 18 of this policy.

5. Antivirus Policy

Antivirus software is installed on all Trust computers and is used to scan local disks, email and network files for malicious software. Should you discover or be alerted to the presence of a virus or other malicious program, you should stop using your computer immediately, disconnect it from the network by shutting it down and remove any portable media from the computers' sockets. You should then alert the IT Technical Support department providing as much information about messages that are displayed.

In addition:

- Do not attempt to interfere with or attempt to stop the Anti-Virus software on your computer;
- Do not attempt to introduce virus code, spam software or other malicious code;
- Removable media such as portable hard drives or memory sticks should be scanned prior to use, especially if they do not belong to the academy or Trust and have been used in equipment that does not belong to, or is otherwise loaned by any of the Trust academies.

The Trust anti-virus systems are updated frequently. If your computer is not connected to the network or home Internet for some time, please ensure the IT Support Department scan the contents before you attempt to use it on the network.

5.1 Passwords and Password Security

In the interest of student and staff security, to protect the integrity of the network and to safeguard the data we hold, **it is vitally important that you do not divulge your credentials to anyone**. Your username and password gives you access to your email account and sensitive information held by the Trust and academies. If you believe your password has been discovered, you should inform the IT Support Department immediately. A member of the technical team will reset your password and inform you of how to change it when you log in.

The Trust IT Systems employ a password policy that requires your password to meet certain criteria before it will be accepted. It will expire after 30 days (for staff, 90 for pupils / students) after which you will be required to input a new one. This must be of suitable complexity:

5.1.1 At least 8 characters long;
5.1.2 Must contain at least 1 upper case letter and one number;
5.1.3 Must not be the same as any of the previous 5 passwords you have used;
5.1.4 Cannot contain contiguous elements of your username.

Please contact the IT Support Department if you need assistance with this process.

Where you access multiple systems (such as the MIS or secure websites) it is good practice to use different passwords for each system. You should also ensure that any username and password required to access elements of a website are not stored by the website. This practice means any systems you currently access are available on your device to whomever uses it when you are logged on.

Be aware that web based systems provided by the Trust should not be accessed from a public or untrusted computer – an Internet Café for example. You should only access these systems from your own personal computer (preferably one which is not used by other family members, particularly children) or from a Trust or Academy owned or loaned device.

5.2 The disposal of Computers and other ICT Equipment

The security of any data that may remain on computers or other ICT Equipment once it is ready for disposal is taken very seriously. All redundant ICT equipment that may have held sensitive data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed it will be physically destroyed. We only use authorised companies who will supply a written guarantee that this will happen and provide a certificate of authenticity and proof once the data has been securely erased. Any data that contains information such as student records, personnel information or financial information is securely erased in addition and prior to being sent for secure disposal.

The IT Technical Support Department maintains a comprehensive inventory of all ICT equipment including a record of disposal. This includes:

5.2.1 Date item disposed;
5.2.2 Authorisation for disposal;
5.2.3 Verification of software licensing removal;
5.2.4 Any personal data likely to be held on the storage media*;
5.2.5 How it was disposed of e.g. waste, gift, sale;
5.2.6 Name of person or organisation who received the disposed item;

Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate in addition to these data security measures

In addition to data protection, and the Electricity at Work Regulations 1999, the disposal of computers and any other ICT equipment conforms to The Waste Electrical and Electronic Equipment Regulations 2013, As indicated in the following websites

https://www.legislation.gov.uk/uksi/2013/3113/contents/made
https://www.hse.gov.uk/waste/waste-electrical.htm

.*If personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

6. Network and Data Access

Access to the Trust ICT network, its data and services is by the use of unique usernames and passwords (hereafter called 'credentials') which identify you on the network. Your credentials allow you access to various features of the network such as the Internet, intranet, email and networked applications the level of which depends on your position within the academy.

This section details the accepted and prohibited use when accessing network-attached devices (collectively known as 'the Trust network' or just 'the network'), the shared data and other applications that affect the use of the network.

6.1 General use of the ICT Equipment

Any Trust or Academy computer that accepts your credentials will allow you access to data, the Internet, email and other IT services. In the main, it is intended that access to the network will be for the specific business of the Trust and Academies during your normal working hours. However, use of the network and devices for non-Trust or Academy activities is acceptable outside of your normal hours of work provided the scope of use does not breach any of the prohibitions listed in this document. You are solely responsible for your activity when logged in to an academy computer and any data saved, transmitted or printed. Access to the network, remote system, the MIS and websites is recorded and may be monitored as set out in section 3.2 of this document)

A great deal of sensitive and confidential information is stored on the network, the majority of which can only be accessed by staff credentials. Should you suspect your username and password have been discovered, you should alert the Trust IT Systems Manager immediately. Abuse of the network and networked systems is considered a serious breach of this policy.

- You should not install, or attempt to install any software not licensed to either the Trust or individual academies. All software should be installed by the IT Technical Support department. Legal entitlement to use the software as requested will be sought before any software is installed. This does not extend to the installation and use of device drivers such as those required to operate personal printers or portable media.
- You should not seek to use, change, misrepresent or distribute other user's data that is stored on the network unless you have explicit written consent from the owner of that data or a legal basis to do so.
- Do not attempt to discover, bypass or tamper with any security feature or setting that applies to either networked devices or devices that use the network but are not directly connected to it. This includes the use of password discovery software and other malicious programmes designed to bypass computer or network security (either directly or indirectly).
- Material that is copyrighted should not be installed, copied, duplicated or transmitted in any way that contravenes the copyright of the material.
- You should not attempt to delete, alter or destroy any data stored on the network, its components or security devices unless that data belongs to you.
- Do not attempt to access the network or any data or component by masquerading as another user unless explicit written permission is granted by that user.
- Do not store information on shared, public areas of the network that could be used to identify individual pupils / students, members of staff or other third parties.
- You should not seek to disrupt access to the network for other users either by the introduction or removal of software or hardware devices.
- Do not allow third parties or other visitors to attempt to access any email system, or plug in any device whilst you are logged in to the computers. Any portable media should be scanned by the IT Support Department before it can be used in an academy computer.
- The Trust, Academies or IT Support Department are not responsible for any data that is not stored on the network. If you do use portable media, make sure you make frequent backups.
- Any data that is considered personal, confidential or sensitive should not be stored on portable media unless the media is encrypted (see section 3.1 Data Security) you are solely responsible for any data that is removed from any academy premises, electronic or otherwise.

7. Internet Access

The Internet is a global communications network that combines many thousands of smaller networks and offers a huge amount of educational content, research material and entertainment websites. It also hosts adult content on-line services and websites that are unsuitable for education environments and some that may be considered objectionable. Every effort is made by the Trust to prevent access to such material by the use of firewalls, content filtering and advertisement blocking software, spy prevention software, anti-virus screening and anti-spam software.

The Internet is not a secure medium and any information uploaded such as personal, bank or financial details, sensitive or confidential information is done so at the users own risk. The Trust accepts no responsibility or liability for any loss or damage that may occur. Furthermore, the Trust will not be liable for any losses or disputes resulting from on-line banking, shopping websites, gambling websites or trading stocks and shares. Users participate in these activities at their own risk and must indemnify the Trust against any claim or demand against them as a result of such activity.

7.2 Using the Internet

You can access the Internet on any computer that is connected to the Trust network. You should be aware however, that Internet use is monitored by the IT Support Department (as laid out in section 3.2) for information on how this affects personal devices that use the Internet via the Aston Academy BYOD (bring your own device) network connections (available only in some academies), please see section 10.0.

To protect your privacy, any websites you access when you are connected to the Trust VPN, are not filtered or monitored. However, accessing information via the Internet in this manner should not contravene these policies where you are using Trust equipment.

It is intended that use of the Internet could include:

- Access to websites that support the business, activities or educational needs of the Trust or individual Academies.
- The use of websites to support:
    - Research;
    - Professional development;
    - Maintaining skills;
    - On-line Examinations.
- Access to download sites for information or data exchange, results data or other student related information. This also relates to uploading information.
- Access to websites that would otherwise contravene this policy but where an ICT Technical Support investigation is required (and only when requested by the Chief Executive Officer (CEO)) either in the interests of child protection, or to enforce this policy. This includes but is not limited to bypassing wholesale security systems designed to filter websites that may be deemed objectionable.
- You can use the Internet for personal use but this is limited to outside your normal working hours (i.e. during lunch or before / after academy) and whilst personal use is permitted at these times, any activity should not contravene the prohibitions listed in this document.

Abuse of Internet access is considered a serious breach of this policy. You are reminded that suspicion of abuse will be monitored in accordance with section 3.2 of this document. Despite the advantages that the Internet brings, you should not access or attempt to access websites, programs or files for the following activities:

- Excessive personal use during your normal working hours.
- You should not use the Internet for private business and/or gain.
- Wilfully and knowingly accessing websites, resources, graphical images or other on-line material that is in breach of the Obscene Publications Act (1964), the Children Act (2004), the General Data Protection

Regulation (UK GDPR), The Human Rights Act (1998), The Computer Misuse Act (1990) or the Copyright, Designs and Patents Act (1988)

- Distributing, publishing or permitting to be displayed any information that would breach The Copyright and Related Rights Regulations 2003, the Obscene Publications Act (1964), the Children Act (2004), the Data Protection Act (1998), The Human Rights Act (1998), The Computer Misuse Act (1990) or the Copyright, Designs and Patents Act (1988)
- Accessing chat rooms or software that launches chat sessions, instant messaging, forum or bulletin boards unless it is for specific educational or technical dialog.
- Social networking or micro blogging unless it specifically relates to the business of the Trust (see section 8.0 Social Media)
- The use of gambling websites (such as on-line bingo or casinos) including betting, odds calculators or accumulator calculator websites.
- Downloading illegal or un-licensed software, compressed image files, web installed applications or peer-to-peer file sharing utilities.
- Uploading content or information to websites or file transfer sites other than for uses specifically defined as acceptable use or where the site belongs to the Trust.
- Knowingly uploading, posting, transmitting, or searching for material that is unlawful, indecent, defamatory, obscene, offensive, abusive threatening or racially motivated.
- Using forum or bulletin boards not specifically designed for educational use or other business of the Trust.
- Uploading, posting, or transmitting personal information such as names, addresses, telephone numbers or financial information of another person without their consent or with no legal basis for doing so.
- Accessing, searching, or receiving any personal information about another person without their consent or with no legal basis for doing so.
- Downloading or transmitting copyrighted material without express consent of the copyright holder.
- Attempting or succeeding to bypass security measures or filtering systems except in authorised circumstances.
- Attempting to disrupt access to the Internet for other users.
- Any activity that is illegal under any jurisdiction.
- Using the Internet to promote otherwise legal material with which the Trust does not wish to be associated in order to protect its reputation and standing or to protect is staff and pupils / students.
- Upload or make available any credentials or settings that would allow access to the IT systems, information or data on the network by persons not authorised during a normal working day to access that information, data or system.

Relating to pupils / students:

Pupils / students should not be allowed to use the Internet unless under direct supervision by staff. You should be aware of the websites and on-line content being accessed by pupils / students and they should only be allowed to use the Internet when directly related to the topic they are working on. This includes some access to video websites such as Youtube and other sites that may be inaccessible under normal circumstances. **Do not allow pupils / students to use a computer that you have logged into using your own credentials.**

Despite filtering software being used by the Trust, new websites and content is continually being uploaded to the Internet. Should an inappropriate website be discovered either as an accidental referral from another site or with intent, you must inform the Trust IT Services Manager immediately so that the site can be blocked.

8. Email Systems

The Trust email system is a communications tool that is accessible from any computer that is connected to the Trust ICT network or other private network if you are not in school, which can be accessed using your personal credentials. This username and password opens your own personal email only.

The Trust email system uses Microsoft Office 365 cloud services and so is available in and outside the Academy sites. It can be accessed by going to www.office.com and using your credentials from the relevant Academy.

8.1 Using the Trust Email Systems

The electronic mail system is to be used primarily for the business purposes of the Trust and academies. You can use this facility for:

8.1.1 Communications within the Trust and each academy either formal or informal.

8.1.2 Formal and informal communications with external recipients on Trust or academy business.

You can use the email system for personal use but any activity should not contravene the prohibitions listed in this document. It should also be noted that the electronic mail system is provided by the Trust and may be monitored in accordance with section 3.2 of this document which may also inadvertently result in the capture of personal email.

You are reminded that suspicion of abuse will be monitored and may be subject to disciplinary action and/or reported to law enforcement agencies. Whilst you can use the Trust email system for personal use, the following items would be deemed in breach of this policy.

8.1.3 Excessive personal use during your normal working hours.

8.1.4 Using your Trust email address to sign up for, or join any newsletter or regular communication not related to the activities of the Trust.

8.1.5 Use or allow your email address to be used to create forum or bulletin board accounts that do not relate directly to the activities of the Trust.

8.1.6 Knowingly transmit any program, code or complete or part-complete software product as an attachment or as part of a message body.

8.1.7 Transmit or knowingly receive any program that could be categorised as virus code, Worm, Trojan or other malicious script or program.

8.1.8 Masquerade as another user when sending messages.

8.1.9 Send, receive, solicit, print copy or reply to:

8.1.9.1 Jokes (text or images) based on race, religion, colour sex, sexual orientation, national origin, disability or age.

8.1.9.2 Any message that is disparaging or defamatory.

8.1.9.3 Sexually orientated images

8.1.9.4 Messages that contain adult material, adult humour or innuendo.

8.1.9.5 Any message that ridicules others based on their race, religion, colour sex, sexual orientation, national origin, disability or age.

8.1.10 Messages that contain links or credentials to websites, forums or bulletin boards that contain material that is in breach of the Obscene Publications Act, the Children's Act, the General Data Protection Regulation (UK GDPR), The Computer Misuse Act or the Copyright, Designs and Patents Act.

8.1.11 Transmit personal or confidential information outside of the Trust without authorisation to do so.

8.1.12 Send electronic chain letters or messages.

8.2 Additional Email Guidelines

As a guide (although by no means exhaustive), the following information should not be transmitted outside of the Trust or any academies unless it is suitably encrypted, the recipient is aware the message is encrypted and

has the means with which to decrypt the message:

8.2.1 Usernames and passwords.
8.2.2 Any data either in the subject line, message body or as an attachment that could identify any individual, member of staff, student or third party;
8.2.3 Any personal information such as bank details, credit or debit card numbers or other financial data;
8.2.4 Any information that relates to any specific educational requirements of pupils / students;
8.2.5 Any information regarding the health or wellbeing of any staff member or student.

Section 4.0 (all parts) deals with the security, use, transmission and retention of data as well as what activities are monitored by the Trust. Email messaging systems usually (and by default) send messages in plain text that is easily read if a mailbox is compromised. To prevent access to such information data of a sensitive nature should be either password protected or encrypted if it is to be sent via email. In addition, there is a risk that any passwords sent (particularly in the same email as the data) may also be easily captured and used to unlock the data. It is recommended that one of the following methods be used to transmit passwords to unlock data you have sent beyond the Trust network:

- Send the email to the address and send the password via SMS
- Send the email to one address and email the password to another that is only accessible by the recipient of the data
- Send the email to the address and make a phone call to pass on the password

If these options are not available, then you could send the password in a separate email but **be aware of the risks of doing so.** If this mailbox is a shared message box for example, or if the mail server or mail account has been compromised and an attacker has access, there is a risk that data could be discovered by someone other than the intended recipient. Any breaches of data security should be reported to the IT Network Manager and/or Data Protection Officer.

Section 3.1 covers some aspects of data security and what process should be followed to transmit or otherwise make data available to third parties. This should be read in conjunction with the ACET GDPR policy and Privacy notices.

Unsolicited (or spam) email is a problem that affects all email systems. The Trust uses software and hardware devices that attempt to filter spam from legitimate email but sometimes these types of messages do avoid the filters and arrive in your inbox. These emails can range from simple annoying messages to malicious code. **As a rule you should never open email if you do not know the sender, nor should you open attachments that you do not know the content thereof**. The guide you received when you collected your laptop from the IT Technical Support department gives guidance on how to access email that may have been quarantined by this service.

9. Cloud Systems

Cloud based systems for the purpose of this document refer to those systems hosted by third-party providers for the purpose of information gathering, sharing and distributing (within the public domain) and for the further purposes of the business of the Trust.

9.1 Google G-Suite

The Trust has implemented the G Suite cloud system from Google for use within academies across the Trust. This gives access to a number of applications that can be accessed easily from home or anywhere where you have an Internet connection. The use of the applications should be for the business of the trust and providing an education platform for pupils / students to access.

The following applications within the G Suite system have been made available during the initial implementation:

- Google Drive
- Google Classroom

- Google Docs
- Google Sheets
- Google Slides
- Google Calendar
- Google Meet
- Google Sites
- Google Contacts
- Google Forms

A number of other applications are available and when evaluated will be published.

Also included with the G Suite system is Google Mail however, email from the existing ACET systems was not migrated during the initial implementation. This remains an additional system and email outside of the ACET G Suite system. Any data stored in this system is not subject to the ACET backup systems and cannot be recovered using our backup and recovery procedures.

9.2 Use of Google Applications

The application within the G Suite systems all have specific terms of service and privacy statements that can be viewed at the following location:

https://policies.google.com/terms

Use of these systems to store and retrieve information falls within the same guidance as when using the ACET on-premises systems and is as laid out in this document. Information that is presented for public consumption (or for pupil / student access in the case of Google Classroom) should meet the same standards as those stored and delivered on the ACET file servers, email systems, websites and social media sites.

10. Mobile Devices

Security and the correct use of mobile equipment throughout the Trust is essential. The Trust uses a number of mobile devices all of which can access information stored on the Trust network including email. The use of mobile smartphones has become increasingly widespread and several devices are used by members of staff on Trust or Academy business. Please note that this policy also applies to mobile equipment that can be used to connect to Internet services outside of the Trust academies. In addition to this policy, the following condition also applies:

- If you are using your Trust laptop to access any of the Trust services (files / email or applications) and you are not connected to the Trust Wi-Fi system then you should always use the VPN connector software initiated by ticking the relevant box when you attempt to log on to your computer. This ensures the connection you make to these services is secure and encrypted. You should always use this method at the time you log on, especially when you are connecting to unsecured, public networks. If the VPN connection box is not present on your Trust laptop then please contact IT Support who will be happy to install this software for you.' **Do not use any third party VPN applications or tools on your ACET laptop other than those provided by IT Support.**

- If you are accessing the Trust email or file access services *whilst using your own devices* connected to unsecured, public Wi-Fi networks then steps should be taken to make sure your connection is secure. Accessing this type of network leaves your device open to a vulnerability known as a MITM (man-in-the-middle) or hijack attack whereby an attacker attempts to intercept the communications between two devices and could lead to disruption of the service or loss of sensitive data. Trust computers can be connected to the network using a secure VPN when at home or outside of the academies which secures any connection and encrypts the data that is transmitted. You can secure your own device using a personal VPN system, generally for a small monthly or annual subscription cost and available for a number of devices including Windows, MAC, Android and Apple

iOS. Norton Secure VPN is one such service although other VPN services are available. These types of VPN will secure all of your network activity, whether that is access to Trust email services or other personal services such as Banking. If the only service you wish to secure whilst connected to unsecured, public networks is access to your Trust email system, then you should download the CudaLaunch application from the ACET website (www.astoncetrust.org/cudalaunch.exe). This application download is only available for Windows devices. For Android and iOS devices the application can be downloaded from the relevant app store (search cudalaunch). If you download this application, please contact IT support for the settings you will need in order for it to connect successfully. Please be aware that there are some VPN services that are not secure and should be avoided, although the names and offers for these companies does change regularly and providing a list of these is difficult. If you wish to use this type of services and are unsure as to which would be best for your needs, please contact IT Support who will be happy to go through the options with you.

- If your device is lost or stolen, we will remotely erase its contents which may result in the loss of personal data. **You must not use your own personal device for Trust or academy business if you do not agree to this potential course of action.**

All members of the teaching staff and some support staff have access to a laptop for their own use. You can use these devices anywhere inside all of the academies and to connect to any Internet system you have at home. Every member of staff that is assigned mobile equipment is required to sign a form accepting the terms of use for that equipment. The form outlines specific use of the equipment which is in addition to this policy. By signing that form, you agree to the terms and conditions with the loan of equipment policy.

You are reminded that this policy also applies to any use of mobile equipment outside of the Trust academies. If you connect your school mobile devices or laptop to your own Internet connection, you are still bound by the terms and conditions laid out in this policy.

11. Social Media

Social Media is a common term given to Internet based services that can be used to share items such as documents, photos and video, items of news or personal information with others that are part of a 'social network' or community. This media outlet includes the building of online communities and encourages information sharing, participation and engagement. The platforms offer up exciting opportunities. However, as the practical application of such technologies by the Trust and its member academies is continually developing, there are many potential issues that should be considered and we should be mindful of the impact the use of such technology may have particularly with reputation, legal and ethical issues.

11 .1 Definition of Social Media

For the purpose of this document, social media is categorised as interactive, online system designed and used for storing, retrieving and sharing information either at a given time or instantly with an online community (either private or public). Current, popular systems include:

- Facebook
- Twitter
- Instagram
- Tumblr
- Flickr
- MySpace
- Pintrest
- TikTok

It should be noted that there are other forms of social media and networking that are not listed here and this is not meant to be an exhaustive list. The development of social media websites, microblogging and other information sharing websites is a constantly changing environment and you should apply the ethos of this policy to any site or community that is generally termed 'Social Media'

11.2 General guidance

This policy should be read in conjunction with the Teachers Standards (parts 1 and 2) – 2011 (updated 2013). Up to date information can be found on the Government website by using the following links:

https://www.gov.uk/government/publications/teachers-standards
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/665522/Teachers_standard_information.pdf

11.3 Use of social media by the Trust or academies

Any use or contribution to any public facing website or social media outlet used by the Trust or any of the trust academies should be in accordance with the standards detailed elsewhere in this policy and should use the same safeguards as any other post, email message, blog or comment posted on chat sessions or forums. In addition, and in all instances, you should:

Remember that any public post will represent the Trust and its academies and posts should be made with the integrity and reputation of the Trust and academies in mind.

11.3.1 Not post information or any image that is a breach of confidentiality either related to Trust or academy business or any confidential information about employees, pupils / students or agents.

11.3.2 Bring the Trust or any academy into disrepute by either making defamatory remarks about individuals or other organisations or criticising the Trust, any employee, group or other individual associated with the Trust or any Trust academy.

11.3.3 Breach copyright by reproducing or posting images (without consent of the owner), failing to acknowledge the work of others, posting in whole or in part any copyrighted information, or information subject to any intellectual property rights without express written permission from the owner of that information.

11.3.4 Not transmit, post, or permit to be posted any information that is unlawful, indecent, defamatory, obscene, offensive and abusive, threatening or racially motivated.

11.3.5 Masquerade as another user or entity when posting messages or other items.

11.3.6 Not post, allow to be posted or transmit any content, information or image that could be construed as bullying, or contains material that is in breach of the Obscene Publications Act, the Children's Act, the General Data Protection Regulation (UK GDPR), The Computer Misuse Act or the Copyright, Designs and Patents Act.

This is not an exhaustive list and a common sense approach should always be made when posting or contributing to social media sites on behalf of the Trust or academy.

Ensure any post that list facts, figures or other information for public consumption is checked by another person to verify the validity of that information before it is posted. You must also check (with the DPO if necessary) that the data you intend to post is authorised for publication into a public forum.

11.4 Using social media in your personal life

The Trust recognises that many employees make use of social media sites in a personal capacity. The Trust acknowledges that employees have the ability to state that they work for the Trust or at one of the Trust academies and also recognises that it is natural for people to discuss their work on social media sites. It is important however, that any discussion with third parties regarding the activities of the Trust or Trust academies be conducted with an official account or authorised person rather than with any personal account.

Whilst personal comments, posts or shared information may not directly be acting on behalf of the Trust or a Trust academy, if they are recognised as being made by a member of staff, any comments or information they post may be misconstrued as coming from the Trust or Trust academies. It is with this view that any opinions offered by individuals where a discussion of work is concerned, should include the line: 'The views I express are entirely my own and do not necessarily represent the views of Aston Community Education Trust, its member academies, agencies or other employees'.

Any content uploaded, posted or transmitted to any social networking or media site should follow the same standards as laid out in this policy for other posts of this kind. You should always use a common sense approach when posting or contributing to social media sites.

The ability for social media websites and services to allow the users to create and develop social communities or 'networks' can be a real benefit when working or socialising in groups. However, it is the advice of the Trust that no member of staff should accept an invitation, nor solicit invitations to join, or be included in the social network or community of any student at any academy governed by the Trust, unless it is on official Trust business, and by using accounts accessible or used by more than one member of staff. You should also not seek to invite to any personal profile, or include in any personal group you are currently an active member of, any account of any student currently attending a Trust academy. This practice should apply to any mechanism, system or service that carries the general term of 'Social Network'.

Further information on the use of privacy settings can be found in the relevant section of the social media website. Some of the more popular sites are listed below:

https://www.facebook.com/help/325807937506242/
https://help.instagram.com/519522125107875
https://twitter.com/en/privacy
https://www.tiktok.com/legal/privacy-policy?lang=en
https://www.messenger.com/privacy
https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en

11.5 Recommended Privacy Settings

To safeguard your own information, and to ensure any information that relates to your privacy remains intact, you should consider enabling security features on any account you create. As a minimum, the following are recommended security level for each potential privacy setting (*note that some or all of these settings may not be available, depending on the service you use*).

Privacy Setting	Recommended Security Level
Send you messages	Friends Only
See your friend list	Friends Only
See your education and work	Friends Only
See your likes, activities and other connections	Friends Only
Your status, photos, and posts	Friends Only
Bio and favourite quotations	Friends Only
Family and relationships	Friends Only
Photos and videos you're tagged in	Friends Only
Religious and political views	Friends Only
Birthday	Friends Only
Permission to comment on your posts	Friends Only
Places you check in to	Friends Only
Contact information	Friends Only
See your current city and hometown	Friends Only

Please be reminded that this policy should be read in conjunction with the Teachers Standards (parts 1 and 2) – 2011 (updated 2013). Up to date information can be found on the Government website by using the following link:

https://www.gov.uk/government/publications/teachers-standards

12. Using your own equipment (BYOD – Bring Your Own Device)

Consumer electronics products such as smartphones and tablets have seen a huge rise in popularity and features over the last few years and are now finding even more uses in the workplace. A number of Trust academies currently deploy a BYOD network that is totally segregated from the main academy network and allows staff and pupils / students to use their own devices to connect to online services independently of the academy network. This type of network offers great flexibility for working but also brings security implications and support issues. This section defines the type of devices that can be used, how you can use the network facility, what the security implications are and what constitutes a breach of the BYOD policy.

By being segregated, this network does not allow access to the main academy network, any files – personal or shared, nor any applications or devices. You can still access your own documents and email.

12.1 Compatible Devices

Any smartphone, tablet, laptop or ChromeBook that is able to use the 802.11n-2009 standard for which you have write access and is capable of connecting to the BYOD Network. This will include most devices produced in the last 5 or 6 years. If you are having difficulty connecting, contact the IT Technical Support Department who will be happy to help you connect your device.

12.2 Acceptable Use

Access is to the BYOD network is given using your ICT network credentials to identify and authorise you on the network. Connection to the BYOD network will only allow you filtered access to the Internet. The filter used is the same as that used for the general ICT Network in that it is designed to eliminate access to objectionable or inappropriate material.

As your device will be connecting to the Internet using the academy's equipment, the same procedures, policies

and terms for using the general academy ICT network also apply to the BYOD network. Please review section 5 and 6 of this document for the terms and conditions of using the Internet and email within Aston Community Education Trust.

12.2 Support and device security

By its very description, BYOD means that the device you use to connect to the academy's networks and systems is your own personal device. As such, and with the exception of helping you connect your device, **we cannot offer any technical support for any aspect of your device, its success or failure to perform a particular function, nor its suitability for accessing the BYOD network**. In addition, security of your device, its content and availability for use cannot be guaranteed to be error free or totally secure from being accessed by other devices. By using the BYOD network with your own devices you accept and acknowledge that at no point will the academy or Trust be liable for any errors, omissions, technical deficiencies, security breaches, loss of data or other technical issue.

Use of your own personal equipment via the Trust and academy BYOD network(s) is entirely at your own risk.

13. Policy Breaches

By using Trust computer equipment, networks, software or systems detailed in this policy you are accepting the terms and conditions it sets out. All staff and pupils / students of Aston Community Education Trust are expected to adhere to the sections in this policy where it is appropriate to them. Serious or repeated breaches of this policy may result in disciplinary action the severity of which will be determined by the Chief Executive Officer (CEO) and / or Academy Trust Directors.

14. Acceptable Use Policies / Codes of Conduct

These policies are aimed at staff, pupils / students and some third party users of the Trust ICT Systems. They are general rules that, in conjunction with this and other policies, define your responsibility when using the Trust ICT Computers and handling data. Staff and pupils / students are required to accept the Terms and Conditions set out in these policies and are reminded of this during the log on process to any Trust or academy computer. By logging onto a Trust or academy computer, they indicate their acceptance of these policies and agree to abide by the terms and condition they set out.

Each policy will be distributed to staff and pupils / students on starting with their academy, updated and re-distributed according to the timeframes set agreed by the Trustees and academy Governing Bodies.

These pages can be printed and distributed for each student / member of staff at the commencement of them starting with the academy
/ Trust or after every review of this policy. Please see section 13 of this policy for information about the renewal process of this document and any associated text.

14.1 AUP Students – Secondary

ICT and Computer Acceptable Use Agreement: Pupils - Secondary

I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes.

- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone.
- I will only use my school e-mail address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- 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 and attended by my teacher.
- Images of students and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network.
- 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.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system or any other computer security system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- 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.

Primary Pupil Acceptable Use

Agreement / E-Safety Rules

- I will only use ICT in school for school purposes.
- I will only use my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

• I will not deliberately use the Internet to search for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.

- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-Safety.

14.3 AUP Staff, Governors and Temporary Users

Staff, Governor and Temporary Users
ICT Equipment Acceptable Use Agreement & Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. This Code of Conduct supplements the E-Safety and Data Security Policy covering the use and procedures associated with all aspect of the Trust IT Computer Network. By using the ICT Equipment within the Trust academies, you agree to be bound by the terms and conditions of this document, a summary of which is detailed below:

- I will only use the school's email / Internet / Intranet / VLE / VPN and any related technologies for professional purposes or during specific time, when it acceptable for personal use.
- I will comply with the E-Safety Policy and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Chief Executive Officer (CEO) or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the IT Technical Support Department.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff, Chief Executive Officer (CEO) or Governing Body.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or the Chief Executive Officer (CEO). I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policies and help pupils to be safe and responsible in their use of ICT and related technologies.

I understand this forms part of the terms and conditions set out in my contract of employment and by using the school ICT Equipment I agree to be bound by this code of conduct and the Trust E-Safety and Data Protection Policies.

15. Legal Issues and Further Guidance

There is a large range of legislation that covers the use of information, ICT equipment, software and the storage and processing of data. Listed below are some of the relevant documents and acts that contain references to the use of ICT:

- The UK General Data Protection Regulation (UK GDPR)
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Privacy and Electronic Communications Regulations UK
- Freedom of Information Act 2000 (there are UK outstanding changes to this legislation)
- ICO Employment Practices Code (not updated for UK GDPR)
- The Copyright and Related Rights Regulations 2003
- Libel Act 1843 (Defamation act 2013)
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994 (there are outstanding changes to this legislation)
- Malicious Communications Act 1998
- Communications Act 2003(there are outstanding changes to this legislation)
- Teachers Standards (parts 1 and 2) – 2011 (updated 2013)

All of these documents are relevant to this policy (in whole or in part) and where possible the document states which legislation is relevant to a particular section. Where a policy is awaiting changes, any up to date information can be obtained by searching for the relevant legislation on the Government website:

https://www.legislation.gov.uk

16. Policy Review

This policy is reviewed annually.

17. Terminology / Glossary of Terms

Throughout this document certain terms are used to describe systems, functions and legal information. Listed below are the terms and meanings used.

802.11n-2009 - is a wireless networking standard that uses multiple antennas to increase data rates.

API: Acronym for Application Program Interface, a set of tools, routines and rules for building software applications in a consistent way.

ASP: Specialist Internet service provider (ISP) that allows a corporate clients to have a software application (e.g. an e-Learning Platform) hosted in exchange for a rental fee.

Authentication: Process of confirming the identity of an individual.

AUP: Acronym for Acceptable Use Policy i.e. agreed procedures in place to minimise e-security and e-safety risks

AVI: Acronym for Audio Video Interleave - the file format used by Microsoft Video for Windows.

Bandwidth: Term that describes how much data can be sent via a connection in a specified time. This measurement is typically described in bps or bits per second.

Bit: The minimum unit of computer data - either a 0 or a 1.

Blog: A blog (a contraction of the term "web log") is a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video.

Bps: Acronym for Bits per second the units in which the speed of communication devices are rated. Indicates the amount of information a device can transmit and receive each second.

Browse: Process of viewing web pages over the World Wide Web.

Browser: Program that allows you to view and interact with web pages on the World Wide Web.

BYOD: Acronym for Bring Your Own Device. The mechanism that allows users to connect to a segregated part of the network for the provision of Internet Access using their own personal devices. This connection method gives no direct access to the resources or services available from the protected network segment that would normally be available when using Trust devices.

Byte: Unit for measuring data - 8 bits=1 byte.

CEOP: The Child Exploitation and Online Protection Centre delivers a multiagency service dedicated to tackling the exploitation of children.

CD: Acronym for Compact Disc. Originally an audio-only format the CD has spawned a range of derivatives including CD-ROM (Compact Disc Read Only Memory), CDi (Compact Disc Interactive) CD-R (CD-ROM Recordable) and most recently CD-RW (Compact Disc Re-Writeable).

Chat: Talking to one person or many people, usually in text format via the internet

Childnet: A non-profit organisation working with others to help make the Internet a positive and safe place for children.

Compression: Reducing the size of a file so that can be transmitted more quickly and takes up less storage space.

Cookie: Small element of data or sent to your computer when you visit a website. When you subsequently return to the site this data may be used for a range of things including recalling your username.

DHTML: Acronym for Dynamic HTML, a way of developing web pages with enhanced functionality. Standards for DHTML are still being developed.

Digital: Made up of zeros and ones (or bits of information)

Distribution Group: A single address that can be used to send email to multiple recipients.

DNS: Acronym for Domain Name System the system that converts computer or domain names into IP addresses either over a local network or the internet. The core of the system is a vast database that stores the names and network addresses of every computer, accessed whenever a computer needs to convert a Domain Name into a numeric IP address

DPA: Data Protection Agency

DPO - Data Protection Officer. A DPO is a person who is given formal responsibility for data protection compliance within an organisation. Under the UK's General Data Protection Regulation (UK GDPR)

Domain:

- In a LAN, a subnetwork made up of a group of clients and servers under the control of one security database.
- In a communications network, all resources under the control of a single computer system.
- On the Internet, a registration category. (Internet Domain Name)
- In a hierarchy, a named group that has control over the groups under it, this may be domain names themselves.
- Email addresses normally consist of a user ID and a domain name separated by the @ symbol

Download: The process of copying files from one remote host to your computer.

DVD: Acronym for Digital Versatile Disc

E-Learning: Wide range of electronic learning applications and processes including Web-based learning, computer-based learning, virtual classrooms and digital collaboration. Commonly held to include delivery of content via Internet, intranet/extranet (LAN/WAN), audio/video tape, satellite broadcast, interactive TV, and CD-ROM.

EEA: European Economic Area. The area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the internal market of the European Union (EU). The EEA was established on 1 January 1994 upon entry into force of the EEA Agreement.

Email: Sending electronic messages over a network or the internet.

Email Client: An application used for sending, receiving and reviewing email.

E-Security: procedures to ensure all electronic data is categorised as public, restricted or protected and that electronic systems containing the data are securely maintained

E-Safety: procedures to ensure computer users know their access rights and responsibilities in using ICT.

Extranet: A local area network (LAN) or wide area network (WAN) using TCP/IP, HTML, SMTP, only available to people inside and certain people outside an organization, as determined by the organization.

FAQ: Acronym for Frequently Asked Questions

Flash: A vector graphic animation tool marketed by Adobe and widely used for developing web delivered e-learning.

FTP: Acronym for File Transfer Protocol. A process that allows you to transfer files or programs to, or from computers across the internet.

GDPR: The General Data Protection Regulation (EU) 2016/679 ("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). Now covered by the UK GDPR from Jan 2021

GIF: Acronym for Graphics Interchange Format, a common format for the storage of largely non-photographic imagery.

Gigabyte: 1024 megabytes of computer data

Hardware: Physical technology such as computers monitors and keyboards rather than software.

Hits: The number of requests for information made to a server.

Host: Another name for your computer. A computer connected to a network is known as a host.

HTML: Acronym for Hypertext Mark-up Language -the basic language that is used to construct web pages. There are several HTML standards in existence.

HTTP: Acronym for Hypertext Transfer Protocol, the standard that regulates the way information is transferred around the World Wide Web.

Hyperlink: Underlined word or set of words that, when clicked, takes you to a different place on that page, alternative website or file for download.

ICT: Acronym for Information and Communication Technology

IT: The technology involved with the transmission and storage of information, especially the development, installation, implementation, and management of computer systems within companies, universities, and other organizations

Internet: A range of networks interconnected via TCP/IP protocol.

IP: Acronym for Internet Protocol, the rules that regulate the way information is transferred across local networks as well as wide area networks such as the Internet.

IP Address: computing internet protocol address: the numeric code that identifies all computers that are connected to the internet, or local area network.

IPS: Acronym for Intrusion Prevention System; a network security device that monitors network and/or system activities for malicious or unwanted behaviour and can react, in real-time, to block or prevent those activities.

ISP: Acronym for Internet Service Provider, companies that provide users with access to the internet.

Intranet: A private network inside an organisation that uses Internet technology. Usually available from any location.

Java: Language developed specifically for creating software that can be simply downloaded from the Internet, but now used for a wide range of applications.

Javascript: Language similar to Java but actually incorporated into web pages in the interests of creating various special effects.

JPEG: Acronym for Joint Photographic Experts Group, the committee that originally developed this special image file format. JPEG files are now the most popular format for storing photographic images on the World Wide Web.

Kilobyte: Unit of computer data, made up of 1024 bytes.

Learning Platform: A Virtual Learning Environment with facilities for communication, work storage and access to learning resources

Learning Portal: Web site that offers learners consolidated access to learning and training resources from multiple sources.

Login: The acts involved in entering a computer system or the account name you have been allocated to gain

access.

Megabyte: Unit of computer data made up of 1024 kilobytes.

MIS: Acronym for Management Information System; provides a co-ordinated approach to the gathering and use of data.

MPEG: Acronym for Moving Picture Experts Group, the committee who devised this innovative file format for storing video images.

Network: Two or more computers connected together.

Offline: Term that implies that an item of hardware or software is no longer actively linked with a local network or the Internet. See Online.

Online: Opposite of Offline i.e. an item of hardware or software is actively linked to a local network or the Internet.

Operating System: The basic system that underpins computer operations and the foundation upon which all other programs operate. MSDOS, Unix and Microsoft's Windows are all examples of operating systems.

Plug-in: Small pieces of software that add to the capability of existing programs.

OWA. A web based application used to view email (see email client).

PDA: An acronym for personal digital assistant which is a mobile device or palmtop computer.

PRIVACY NOTICE: A statement or legal document (private law) that discloses some or all of the ways a party gathers, stores, uses and discloses customer or client information.

POP: Acronym for Post Office Protocol or Point of Presence; the location where connections to a network or the Internet may be accessed via dial-up networking

Remote Access: Accessing and/or processing data from a computer in a different location.

Router: Mechanism (usually hardware) for transferring data between one or more networks.

SCORM: Acronym for the Shareable Courseware Object Reference Mode standard developed by ADLNet

Server: Both the software and hardware that is used to provide access to resources such as software, applications and the Internet.

SMTP: Acronym for Simple Mail Transport Protocol. The almost ubiquitous standard that governs how email is sent and received.

Software: The files, data and programs that allow a computer to function but have no physical dimensions. By way of contrast see Hardware.

Stratum: stratum levels define the distance from a reference clock. Using network protocols, onsite servers synchronise their time with Stratum-1 devices. This generally has a 10 microsecond accuracy over UTC (Universal Time +00:00 GMT in the UK)

System Administrator: An overall administrative account that has full access to all network resources. Also the title for a person responsible for the administration, management and maintenance of computers, networks and software.

Terabyte: Unit for an amount of computer data, consisting of 1024 gigabytes.

Twitter: This is a free social networking and micro-blogging service that enables its users to send and read messages known as tweets. Tweets are text-based posts of up to 140 characters displayed on the author's profile page and delivered to the author's subscribers who are known as followers.

Unix: Operating system for mainframe computers originally designed in the 1960s but still widely used worldwide.

Upload: Send files to another computer.

URL: Acronym for Universal Resource Locator otherwise known as the address of a website.

VoIP: Acronym for Voice over Internet Protocol, or using a local network or the Internet to transmit voice conversations, a technique used within virtual classroom systems and office telephony.

Virus: Self-replicating software that propagates itself from one computer system to another, normally devised with malicious or mischievous motives.

VLE: Acronym for Virtual Learning Environment (See Learning Platform)

VPN: Acronym for Virtual Private Network which is a software application to create a private computer link between computers in different locations.

Web space: Amount of data capacity available for the construction of web pages, normally measured in megabytes.

Website: Collection of linked web pages with a common theme, created for the same purpose.

World Wide Web: A global information resource made up of interconnected web pages.

18. Request for IT Investigation

This form will be completed by the IT Department in all instances where an investigation into e-safety policy breaches or IT Safeguarding issues regarding pupils/students is raised.

Request for IT Investigation

This form should be completed where a request has been made for IT to conduct an investigation into any of the following scenario:

Breach of security
Breach of e-safety policy element
Requests for a review of student activity when using IT equipment that may include a safeguarding concern.
Workplace monitoring of web or email activity
Requests for access to email accounts of third parties

An investigation of this nature should only be conducted with prior consent from the Principal of the academy. You should seek this approval before you commence to section 2 of this procedure.

Please ensure you read the requirements regarding the conducting of IT service investigations in the relevant section of the Trust e-safety policy before you start section 2 of this procedure.

* Required

1. Email *

2. Name of IT Engineer conducting this investigation *

3. Type of investigation requested *

   Mark only one oval.

   - ( ) Breach of security
   - ( ) Breach of e-safety policy
   - ( ) Request to review Pupil / Student activity (potential safeguarding requirement)
   - ( ) Workplace monitoring
   - ( ) Request for access to email account

4. Name of person requesting this investigation *

5. Date requested *

   Example: January 7, 2019

6. Time requested *

   Example: 8:30 AM

7. Does this event involve any pupils / students? If so, list the user account of the pupil / student but no other personal details.

8. If this request involves a pupil / student have the IT Manager and safeguarding leads for the pupil / students home academy been notified?

Mark only one oval.

- Yes
- No
- Other:

9. Description of the request *

10. IT Systems Affected (list all affected systems) *

11. Please note all of the details that have been passed to you by the requester to initiate this investigation. *

12. Have you attended any meetings regarding this event? *

If so, please include the date, time, attendees and any notes you have made from this meeting. Please also attach any supporting documents that you have been given.

13. Use this section to add your supporting documentation from section 1.

You can only update a maximum of 10 files and the largest file size is 10mb

Files submitted:

14. Please confirm you have the authority to continue the investigation before you move to the next section *

Mark only one oval.

- Approval Received

Section 2

Please detail in this section the investigation you have carried out in respect of the request detailed in section 1 of this form. You should include ALL of the following information:

The date and time you started the investigation
The systems you inspected and what elements of those systems you accessed in order to gather your information
Any evidence you found to support the request for an IT investigation, including details of security systems you reviewed, or personal information you uncovered such as IP addresses, website access, usernames or any other

15. Please give an account of the investigation you have conducted.

Ensure you include any files that support your investigation. Include the names of people you have passed information to and the dates and times you handed this information over. If this is an IT related safeguarding issues, please ensure there are at least two members of the IT team present if you need to review any personal information about pupils / students or if you need to conduct any online activity that requires the removal of filtering systems that would breach the e-safety policy on restricted websites.

16. Use this section to add your supporting documentation from section 2.

You can only update a maximum of 10 files and the largest file size is 100mb

Files submitted:

19. Acceptance

You are reminded that by logging into and using the ICT Network Facility or Trust / Academy computers you agree to be bound by the terms and conditions that this document sets out. You are further reminded of this statement each time you boot any computer connected to the trust or academy networks.

Please make sure you read and understand this document in full before you log into any of the Trust or Academy computers.