Co-op Academy
North Manchester

Co-op Academy North Manchester

Name	**E-Safety Policy**
Approved by	**SSCC Committee**
Policy Created	**Nov 2014**
Review	**Annually**
Update Approved	**September 2019**
All policies are available to stakeholders either on the Academy website or upon request from the Academy's Main office.	

1. Aim

1.1 The Academy believes in educating all in the academy community on how using technology effectively as it is a key part of life-long learning and employment. The academy was recognised for its commitment to E-Safety as it is has been awarded the 360 E-Safety award.

This policy should also be read in conjunction with the Trust Code of Conduct policy which also covers aspects of Electronic Communications relevant to staff members.

1.2 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.

1.3 Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting/Streaming
- Music Downloading/Streaming
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Tablets and other mobile devices with web functionality

1.4 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 a minimum age, usually 13 years, which is especially true in the case of social media platforms such as snapchat and Facebook. Whatsapp is only available for 16 year olds.

1.5 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.

1.6 We 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, and potentially damage the reputation of the Academy. This is covered via the GDPR policies and all staff are trained in their understanding of GDPR.

1.7 Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling are made aware of the risks and threats and how to minimise them. All staff

	have undergone relevant training such as e-Safety, Prevent and GDPR.
1.8	This policy is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, smartphones, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, smartphones and portable media players, etc "Bring Your Own Device" (BYOD)).

2.	**Monitoring ICT**
2.1	Monitoring Authorised ICT staff may inspect any ICT equipment owned or leased by an Academy at any time without prior notice. ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, files, e-mails, instant messaging, computer or internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Academy business related information; to confirm or investigate compliance with Academy policies, standards and procedures; to ensure the effective operation of Academy ICT; for quality control or training purposes; to comply with a Subject Access Request under GDPR Legislation or to prevent or detect crime.
2.2	ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, or account folder of someone who is absent in order to deal with any business-related issues retained on that account. This will be under the direction of The Principal (or The Chair of Governors if relating to The Principal). The Principal will then decide whether any other member of the academy should have access to these emails.
2.3	All monitoring, surveillance or investigative activities comply with the relevant legislation and are covered under the Trust policy.
2.4	Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded. Breaches and incident reporting, a breach or suspected breach of policy by an employee, contractor or pupil may result in the temporary or permanent withdrawal of Academy ICT hardware, software or services from the offending individual.
2.5	Any policy breach is grounds for disciplinary action in accordance with the Academy's Disciplinary Procedure Policy breaches may also lead to criminal or civil proceedings.
2.6	Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the academy's e-Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including passwords), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the e-Safety Coordinator.
2.7	Please refer to the section below on Incident Reporting, e-Safety Incident Log & Infringements.

3.	**Acceptable Use**
3.1	The academy has acceptable user polices for both staff and students who are reminded about our conduct when using ICT within the academy.
3.2	Malware All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB memory stick) must be checked for any viruses using academy provided anti-virus software before using them.
3.3	Never interfere with any anti-virus software installed on school ICT equipment that you use.
3.4	If your machine is not routinely connected to the school network, you must make provision for regular virus updates through IT Services.
3.5	If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the IT Services team immediately. IT Services will advise you what actions to take and be responsible for advising others that need to know.
3.6	Never open an email attachment unless you are sure of its origin – even if it looks plausible. If in doubt: delete. Genuine emails can always be resent.
3.7	Signs of possible malware infection include:

	• browser pop-ups; • redirected home page or search pages (i.e. not what you are used to); • sudden, abnormally poor performance (although this may be caused by a number of factors); • alarming warnings from software you haven't come across before. If you are in doubt – speak to a colleague or member of the IT Services team.
3.8	In the event of a suspected virus or other malware infection, the following procedure should be followed: • immediately notify IT Services of the suspected incident; • switch off the equipment and, where practical, warn other users of the possible issue; • remove any writable, removable media from the machine and pass this to IT Services. IT Services will then: • isolate the machine and removable media from the network; • run an updated, stand-alone virus removal tool on the suspected machine and media; • verify the state of virus protection on the main servers; check the state of the infection on the suspect hardware and either: return it to the network / user if virus removal has been successful or; re-install / re-image / re-format the device if the removal cannot be confirmed.

4.	**Email**
4.1	The use of e-mail within the academy is an essential means of communication for both staff and pupils. However, there are specific expectations of the use of emails which are in both the staff handbook and the code of conduct.
4.2	In the context of school, e-mail should not be considered private – Freedom of Information requests may include email trails, for instance.
4.3	Educationally, e-mail can offer significant benefits for instance direct written contact between schools on different projects, be they staff based or pupil based, within school or international.
4.4	We recognise that pupils need to understand how to style an e-mail in relation to their age and intended recipient.
4.5	See the separate GDPR policy for further details and guidance.

5.	**Managing email**
5.1	The academy gives all staff (and pupils) their own e-mail account to use for all academy business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
5.2	It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The academy email account should be the account that is used for all academy business.
5.3	Under no circumstances should staff contact pupils, parents or conduct any academy business using personal e-mail addresses. Staff should never use pupils' personal email addresses under any circumstances.
5.4	All e-mails should be written and checked carefully before sending, in the same way as a letter written on headed paper.
5.5	All pupil e-mail users are expected to adhere to the generally accepted rules of etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication or arrange to meet anyone without specific permission.
5.6	Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
5.7	Staff must inform the Assistant Vice Principal who has responsibilities for e-Safety, their line manager, and the Principal if they receive an offensive e-mail.
5.8	Pupils are introduced to e-mail as part of the ICT or Computing Scheme of Work.
5.9	However, you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

6.	**Sending emails**
6.1	Email is an insecure medium. It should not be used for sending personally identifiable or sensitive information. If you need to send such information within the academy, please store the information on the network and simply indicate to the recipient where the information may be found. Any information which is potentially sensitive should be password protected and ideally, a secure email transfer system, such as egress should be used. (See GDPR guidance and training).
6.2	Use your own academy e-mail account so that you are clearly identified as the originator of a message.
6.3	Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
6.4	Do not send or forward attachments unnecessarily. Whenever possible, send the location on a shared drive / online folder rather than sending attachments.
6.5	Academy e-mail is not for personal use – and will no longer be available once you leave the academy's employment.
6.6	Any member of staff can send an email at any time that is suitable to them, however, they should not expect an immediate response. This is part of our flexible working and wellbeing approach.

7.	**Receiving emails**
7.1	Check your e-mail regularly. The communications policy outlines that emails from parents/carers are responded to within 48 working hours.
7.2	We encourage you to activate your 'out-of-office' notification when away for extended periods.
7.3	Never open attachments or click on links from an untrusted source. If in doubt delete.
7.4	All staff members are reminded that although they may receive emails outside of their working hours, they are not obliged to open or read it. All staff should have due regard to their and others' wellbeing when email medium is being used

8.		**E-Safety roles and responsibilities**
8.1		**Roles and Responsibilities**
	8.1.1	As e-Safety is an important aspect of strategic leadership within the academy, the Principal and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The academy will nominate a named e-Safety coordinator, the Assistant Vice Principal who oversees this area, who will be designated this role. All members of the academy community must be made aware of who holds this post. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.
	8.1.2	Senior Management and Governors are updated on e-safety issues which are relevant and governors have an understanding of the issues and strategies at the academy in relation to local and national guidelines and advice.
	8.1.3	This policy, supported by the academy's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole community.
8.2		**e-Safety in the Curriculum**
	8.2.1	ICT and online resources are increasingly used across the curriculum. It is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis.
	8.2.2	e-Safety is embedded within the curriculum and academies must continually look for new opportunities to promote e-Safety.
	8.2.3	The academy has a framework for teaching internet skills in ICT or Computing lessons and as part of the PSHE programme of study – for instance CEOP resources (covering Internet safety, cyber bullying and related issues) may be embedded in the curriculum and delivered to all year groups. The academy also invites external partners to deliver drop down sessions to pupils to educate them about key safeguarding updates.
	8.2.4	Educating pupils on the dangers of technologies that may be encountered outside the academy is done informally when opportunities arise and as part of the e-Safety curriculum.
	8.2.5	Pupils are taught about copyright, creative commons and respecting other

		people's information, safe use of images, taking and recording of pictures and videos, etc through discussion, modelling and activities as well as the impact of their digital footprint, how and when to seek support.
	8.2.6	Pupils must be aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button, in addition to local solutions such as the "Sharp System." Sessions for parents/carers on e-safety are also delivered through parent/carer forums and through other opportunities such as parents' evenings.
	8.2.7	Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
	8.2.8	The academy has Digital Leaders who play an important part in helping pupils understand how to keep themselves safe as well as producing assemblies, they meet weekly and undertake training from Childnet on being a positive role models in the academy. There is also a clear anti-bullying policy.
	8.2.9	The academy has reviewed its teaching of e-safety in the curriculum using the DfE 2019 guidance – Teaching Online safety in school. We believe that pupils must be taught the underpinning knowledge and behaviours that can help them navigate the online world both safely and confidently, regardless of device, platform or app.
	8.2.10	This policy should be read in line with the RSE and Health Education Policy. This policy outlines the academy's intent to implement a curriculum which also teaches pupils about online safety and harms alongside positive, healthy and respectful online relationships and behaviours.
	8.2.11	As the online world develops and changes quickly, it means that it can make it difficult for the academy to be able to keep up to date with all the latest devices, platforms, apps, trends and related threats. With this in mind, the academy will include in its teaching the underpinning knowledge and behaviours that can help pupils navigate the online world safely. These will include: • How to evaluate what they see online so that they do not automatically see online content as true, valid or acceptable. • How to recognise techniques used for persuasion or manipulation so that they become less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity. • Online behaviour so that pupils understand acceptable and unacceptable online behaviour and that our values should not waiver depending on whether we are on or offline. We will also teach pupils to recognise unacceptable behaviour in others and be confident to report it or seek help if necessary. • Being able to identify online risks and how to act focusing not on do's and don'ts' but on how to assess a situation, think through consequences and decide on the best course of action. • Be able to understand how and when to seek support. • How online content can affect wellbeing including self-image, identify, online reputation, bullying, health, wellbeing and lifestyle
	8.2.12	The academy acknowledges that some groups of pupils are more vulnerable that others e.g. pupils with SEND and will tailor its approach most effectively.
	8.2.13	If during the curriculum, any concerns are raised of a potentially safeguarding basis, then safeguarding procedures will be followed.
8.3		**E-Safety skills development for staff**
	8.3.1	Staff receive regular information and training on e-Safety issues in the form of INSET training and updates, together with this e-safety policy.
	8.3.2	New staff receive information on the school's acceptable use policy as part of their induction. All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
	8.3.3	All staff are encouraged to incorporate e-Safety activities and awareness within

		their curriculum areas.
	8.3.4	Endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
	8.3.5	The e-Safety policy is introduced to the pupils at the start of each school year. The digital Leaders also inform parents through parent/carer evening and parent/carer forums during the course of the academic year.
8.4		**Incident reporting, e-Safety incident log and infringements**
	8.4.1	Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the academy's e-Safety Co-ordinator and the Principal. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must also be reported. This is also in line with our code of conduct, safeguarding and GDPR policies.
8.5		**e-Safety incident log**
	8.5.1	Any incidents will be recorded by the e-Safety coordinator (administrative support available) in the e-Safety log, stored securely in a documented location on the academy's network – the layout of which is presented below: • Date & Time Name of pupil or staff member • Gender Room and computer or device identifier • Details of incident (including evidence) • Actions and reasons Necessary steps will then be taken to investigate this either through Year teams/Safeguarding Leads for pupils, or through the Principal (or a named investigating officer acting on their behalf) for staff. E-Safety log is consistently monitored and evaluated to ensure pupil safety and follow ups are actioned. Incidents are logged on CPOMs, as appropriate.

9.		**Misuse and infringements**
9.1		**Complaints**
	9.1.1	Complaints and/ or issues relating to e-Safety should be made to the e-Safety co-ordinator or Principal. Incidents should be logged and procedures followed.
9.2		**Inappropriate Material**
	9.2.1	All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Principal or Designated Safeguarding Lead.
	9.2.2	Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Principal (or investigation officer designated by them), immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see below). The academy's disciplinary policy will be followed.
9.3		**9.3 Managing an e-Safety incident -** (see flowchart at the end)

10.	**Internet Access**
10.1	The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

11.	**Managing the internet**
11.1	The academy will provide pupils and staff with supervised access to Internet resources (where reasonable) through the academy's fixed and mobile internet connectivity.
11.2	Staff must preview any recommended sites or online systems before use.
11.3	All users must observe software copyright at all times. It is illegal to copy or distribute academy software or software from other sources.

11.4	All users must observe copyright of materials from electronic resources – information made available online cannot be assumed copyright free.

12.	**Internet use**
12.1	You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
12.2	Do not reveal names of colleagues, pupils or others, or any other confidential information acquired through your job on any social networking site or other online system. GDPR guidance must be adhered to at all times
12.3	On-line gambling or gaming is not permitted.

13.	**Infrastructure**
13.1	Details of the local infrastructure, the filtering and safeguarding measures in place are available from the network manager

14.	**Prevent duty**
14.1	Guidance on the Counter-Terrorism and Security Act 2015 – to have due regard to the need to prevent people from being drawn into terrorism (a.k.a. “Prevent”) – explicitly states that: ‘Specified authorities will be expected to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering.’
14.2	While this duty does not confer new functions on any specified authority, ‘the term “due regard” as used in the Act means that the authorities should place an appropriate amount of weight on the need to prevent people being drawn into terrorism when they consider all the other factors relevant to how they carry out their usual functions’. Hence there is an expectation to pay specific attention to the filtering of sites which could be seen as likely to draw young people into terrorism, or to extremist ideologies.
14.3	The Academy therefore ensures that filtering and monitoring systems are able to trap sites and material likely to be covered by the Act. Where a pupil is found to be accessing such material without legitimate purpose (e.g. as part of a Citizenship assignment), it will be treated as a safeguarding issue and reported through the safeguarding processes and uploaded to CPOMs. (See separate policy).

15.	**Social media (and other “web 2.0” technology)**	
15.1	Online technology, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. Behaviour for learning and anti-bullying policies will be implemented for any breaches to this policy.	
15.2	**Pupils**:	
	15.2.1	All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
	15.2.2	Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
	15.2.3	Pupils are always reminded that they must not be giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
	15.2.4	Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
	15.2.5	Pupils are encouraged to be wary about publishing specific and detailed private

		thoughts online
	15.2.6	Our pupils are asked to report anything which causes them concern (e.g. incidents of bullying, inappropriate requests for contact) to the school or a trusted adult or CEOP.
	15.2.7	In extreme cases, where a pupil feels threatened or at risk, the pupil should immediately contact the academy's Designated Safeguarding Lead and procedure will be followed.
	15.2.8	Pupils must not use public social media for school business without the knowledge of the e-Safety Coordinator. Pupils are not permitted to set up any accounts that use the school name or logo. Any incidents will be reported to the Trust's brand team.
	15.2.9	The academy will create a culture that incorporates the principles of online safety across all elements of school life, that proactively engages staff, pupils, parents/carers, that extends online safety principles and models these consistently.
15.3	**Staff:**	
	15.3.1	Staff may only create blogs, wikis or other online systems in order to communicate with pupils using systems approved by the e-Safety Coordinator.
	15.3.2	We do not permit any use of Facebook or other social media sites to engage with pupils for social purposes but may allow access to such sites by individual approval and agreement with the e-Safety Coordinator (with controls introduced to minimise opportunity for abuse) for educational purposes (within the terms set out by the site which may prohibit such use).
	15.3.3	Do not talk about your professional role in any capacity when using social media.
	15.3.4	The e-Safety coordinator must be informed of any blogs created or endorsed by members of staff for use with pupils. These blogs must either require passwords or moderation before posts can be added.
	15.3.5	Staff must ensure that all posts made on social networking sites, whether inside or outside of the academy, reflect the high professional standards expected by the academy and the Trust and adhere to their policies.
	15.3.6	Staff must not use social networking sites as a forum to make derogatory comments which could bring the academy into disrepute, including comments about members of the academy community or the Trust. Any incidents will be dealt with in accordance with the Code of Conduct and Disciplinary policies.
	15.3.7	Staff are expected to demonstrate honesty and integrity and uphold public trust and confidence in respect of anything placed on social networking websites.
	15.3.8	Staff must ensure that any content shared on any social networking website, at any time, would be deemed as appropriate. Staff are personally responsible for ensuring that any privacy settings meet this requirement.
	15.3.9	Staff must ensure appropriate language is used at all times for any comments placed on social networking sites.
	15.3.10	Staff must ensure that any communication and/or images, at any time, could not be deemed as defamatory or in breach of any relevant legislation.
	15.3.11	Friend requests (or equivalent) from pupils must be declined. This includes staff who have left the academy or pupils who have left the academy and are still within school/education leaving age. This must be reported to the Designated Safeguarding Lead and the Principal
	15.3.12	Staff must not establish contact with pupils through their personal social networking sites, or any other means of electronic communication (including personal email or telephone). All contact with pupils must be directly concerned with the pupils' education.
	15.3.13	Staff must refrain from contacting former pupils via personal email or social media. (See 15.3.11). Any emails must come through the school email system.
	15.3.14	Staff should exercise caution in the use of social media where their "digital social circle" (i.e. Friends, Followers, etc) may include other members of the academy community, particularly parents/carers. Be aware that this may lead to indirect communication with pupils – it may be prudent to "unfriend" such individuals or at least inform a line manager via email of any such connections.
	15.3.15	Staff must not publish photographs, videos or any other types of image of pupils or their families on personal social networking accounts, or school

		accounts where permission for publication of images has not been granted.
	15.3.16	Staff must not associate themselves to other businesses or similar online that mentions or links to the academy or suggest that the academy is endorsing the other business or similar.
	15.3.17	Staff are not allowed to set up accounts which use the academy name, the Co-op name or any associated logos.

16.	**Parental involvement**
16.1	We believe that it is essential for parents/ carers to be fully involved with promoting e-Safety both in and outside of school and also to be aware of their responsibilities.
16.2	We regularly consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.
16.3	Parents/ carers are asked to read through the acceptable use policy in the pupil planner
16.4	Parents/ carers / pupils are required to make a decision as to whether they consent to images of their child/them being taken/ used in the public domain (e.g., on academy website)
16.5	The academy disseminates information to parents/carers relating to eSafety where appropriate in the form of eg Information evenings, leaflet drops, Website postings, Email or Twitter

<table>
<tr><th><b>17.</b></th><th colspan="2"><b>Academy owned ICT equipment (also see data protection section)</b></th></tr>
<tr><td><b>17.1</b></td><td colspan="2">As a user of IT, you are responsible for any activity undertaken on the academy’s ICT equipment provided to you.</td></tr>
<tr><td><b>17.2</b></td><td colspan="2">The academy logs IT equipment issued to staff and record serial numbers as part of the academy’s asset register.</td></tr>
<tr><td><b>17.3</b></td><td colspan="2">Personal or sensitive data must not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.</td></tr>
<tr><td><b>17.4</b></td><td colspan="2">A time locking screensaver is applied to all machines. Please lock your machine when you move away from it – even momentarily.</td></tr>
<tr><td><b>17.5</b></td><td colspan="2">Privately owned ICT equipment may only be connected to the Wi-Fi network – contact your IT Services team for further guidance.</td></tr>
<tr><td><b>17.6</b></td><td colspan="2">On termination of employment, resignation or transfer, return all IT equipment to your Manager. You must also notify IT Services so that accounts can be disabled.</td></tr>
<tr><td><b>17.7</b></td><td colspan="2">All IT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:</td></tr>
<tr><td></td><td><b>17.7.1</b></td><td>Liaising with IT Services to ensure compatibility and to benefit from the Academy’s purchasing schemes.</td></tr>
<tr><td></td><td><b>17.7.2</b></td><td>maintaining control of the allocation and transfer within their Unit.</td></tr>
<tr><td></td><td><b>17.7.3</b></td><td>recovering and returning equipment when no longer needed.</td></tr>
<tr><td></td><td><b>17.7.4</b></td><td>All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and and GDPR.</td></tr>
</table>

<table>
<tr><th><b>18.</b></th><th colspan="2"><b>Portable and mobile ICT equipment</b></th></tr>
<tr><td><b>18.1</b></td><td colspan="2">This section covers such items as laptops, mobile phones, tablets and removable data storage devices. Please refer to the data protection policy document when considering storing or transferring personal or sensitive data.</td></tr>
<tr><td><b>18.2</b></td><td colspan="2">All activities carried out on academy systems and hardware will be monitored in accordance with the general policy:</td></tr>
<tr><td></td><td><b>18.2.1</b></td><td>Ensure portable and mobile IT equipment is made available as necessary for antivirus updates and software installations, patches or upgrades.</td></tr>
<tr><td></td><td><b>18.2.2</b></td><td>The installation of any applications or software packages must be authorised by the IT Services team, fully licensed and only carried out by IT Services.</td></tr>
<tr><td></td><td><b>18.2.3</b></td><td>In areas where there are likely to be members of the general public, portable or mobile IT equipment must not be left unattended and, wherever possible, must be kept out of sight.</td></tr>
</table>

	18.2.4	Portable equipment must be transported in its protective case if supplied.

19.	**Mobile technologies**
19.1	Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for pupils.
19.2	Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in the academy is allowed.
19.3	See the relevant GDPR policies and local addenda for further details.

20.	**Bring Your Own Device (BYOD)**	
20.1	The academy allows staff to bring in personal mobile phones and devices for their own use.	
	20.1.1	Pupils are allowed to bring personal mobile devices/phones to the academy but must not use them for personal purposes within lesson time unless under the direct supervision and instruction of teachers. At all times the device must be switched onto silent unless specific teacher permission has been given. Personal phonecalls or messaging should not be made during the day. Pupils are not allowed to video incidents within the academy and post these to sites or store these on their phone. This will be dealt with under the Behaviour Policy.
	20.1.2	This technology may be used, however for educational purposes, as mutually agreed with the e-Safety coordinator. The device user, in this instance, must always ask the prior permission of the bill payer.
	20.1.3	It is the responsibility of the device owner to ensure the device is suitably charged and in good working order.
	20.1.4	Where devices are required for lessons, the academy will make devices available for loan as an alternative to BYOD.
	20.1.5	The academy is not responsible for the loss, damage or theft of any personal mobile device.
	20.1.6	The sending of inappropriate communication between any members of the academy community is not allowed.
	20.1.7	Permission must be sought before any video, image or sound recordings are made on these devices of any member of the school community.
	20.1.8	Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
	20.1.9	Devices used in lessons must be connected to the academy's own filtered Wi-Fi in such a way that the user of the device may be identified so that appropriate filtering policy may be applied and monitored. The academy cannot be responsible for web sites or services accessed through other forms of mobile internet access (e.g. 3/4G connections).
	20.1.10	Mobile internet sharing / hotspots should be disabled as they can interfere with the academy's own Wi-Fi connection.

21.	**Academy provided mobile devices (including phones)**
21.1	Mobile Device Management software should be installed onto all academy owned portable devices for management and monitoring.
21.2	The sending of inappropriate communication between any members of the academy community is not allowed.
21.3	Permission must be sought before any video, image or sound recordings are made on the devices of any member of the academy community.
21.4	Where the academy provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

22.	**Systems access**
22.1	You are responsible for all activity on academy systems carried out under any access/account rights assigned to you, whether accessed via academy IT equipment or your own hardware.
22.2	All access to IT systems and the internet must be via approved systems which provide appropriate management, filtering and security – users (staff or pupils) must not attempt to circumvent these measures for any reason. If in doubt, contact your local IT Services.
22.3	Do not allow any unauthorised person to use academy IT facilities and services that have been provided to you.
22.4	Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time.
22.5	Do not introduce or propagate viruses.
22.6	It is imperative that you do not access, load, store, post or send from academy ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the academy or which may bring the academy, Trust or LA into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the academy's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the equalities Act and other relevant policies).

23.	**Telephone services**	
23.1	You may make or receive personal telephone calls provided:	
	23.1.1	They are infrequent, kept as brief as possible and do not cause annoyance to others.
	23.1.2	They are not for profit or to premium rate services.
	23.1.3	They conform to this and other relevant academy policies.
23.2	Academy telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.	
23.3	Ensure that your incoming telephone calls can be handled at all times	

24.	**Mobile phones & other portable devices**
24.1	You are responsible for the security of your academy mobile phone or device.
24.2	Report the loss or theft of any academy mobile phone or device immediately – the academy remains responsible for all call costs until the phone is reported lost or stolen.
24.3	You must read and understand the user instructions and safety points relating to the use of your academy mobile phone prior to using it.
24.4	Academy SIM cards must only be used in academy provided mobile phones.
24.5	Academy mobile phones may be barred from calling premium rate numbers and any numbers outside of the UK.
24.6	You must not send text messages to premium rate services
24.7	You must reimburse the academy for the cost of any personal use of your academy mobile phone. This includes call charges incurred for incoming calls whilst abroad unless for academy business. (Please see the mobile phone policy)

Appendix

Local infrastructure: The Academy has an up to date monitoring solutions where web-based activity is monitored and recorded.

Staff and pupils are aware that school-based computer and internet activity can be monitored and explored further if required.

If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility, nor the IT Services team's, to install or maintain virus protection on personal systems. Free malware protection for Microsoft Windows (version 7 onwards) may be obtained from www.microsoft.com by searching for "Security Essentials."
Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from network manager
If there are any issues related to viruses or anti-virus software, the network manager should be informed
If you require a site that is normally blocked to pupils open in an IT suite or on mobile internet devices this must be raised with the IT Services in a timely manner (i.e. with at least 24 hours' notice)

Definitions
Here are some definitions of terms used throughout the document for clarity.
Term Brief definition
BYOD "Bring Your Own Device" – general term covering the use of non-Academy devices on the Academy network.
Data Information in the form of text, numbers, scores, images, video, etc (pretty much anything which may be stored electronically)
Encryption Turning data (e.g. text, images, etc) into "code" which cannot be turned back into the original data without the use of a "key" (usually a password of some kind)
IAO Information Asset Owner (see Data Protection Policy)
LADO Local Authority Designated Officer
Malware Generic term for any software intended to do something undesirable. This includes viruses (which spread from machine to machine) and spyware (which surreptitiously collects information).

MARAT Multi Agency Referral and Assessment Team

MASH Multi Agency Safeguarding Hub

Personally, identifiable data Data relating to a (living) individual who can be identified from those data (or other information likely to be available) and includes opinions or what is intended for them (e.g. report comments or assessment scores). Note this includes any class list containing any kind of data.

Portable device Any piece of hardware which is intended to be removed from the school site. Includes laptops, mobile phones, tablets and memory sticks.

Sensitive data Any information which could be harmful if it were to find its way into the public domain. This includes (but is not limited to): personally, identifiable data, confidential information about individuals, the school, or Trust, commercially confidential information such as financial details, etc.