MANCHESTER CREATIVE AND MEDIA ACADEMY

Name	**e-Safety Policy**
Approved by	**SSCC Committee**
Policy Created	**Nov 2014**
Review	**1 year**
Update Approved	**September 2016**
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.

1.2 Information and Communications Technology covers a wide range of resources including; webbased 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.

1.5 We understand the responsibility to educate our students on eSafety 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.

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.

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 students 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 the Data Protection Act 1998, 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.

2.3 All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

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 student 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 eSafety 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 eSafety Coordinator.

2.7 Please refer to the section below on Incident Reporting, eSafety Incident Log & Infringements.

3. Acceptable Use

3.1 Acceptable use policies for students and staff are in use. 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.

3.2 Never interfere with any anti-virus software installed on school ICT equipment that you use.

3.3 If your machine is not routinely connected to the school network, you must make provision for regular virus updates through IT Services.

3.4 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.

3.5 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.

3.6 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.

3.7 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: o return it to the network / user if

virus removal has been successful or; o 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 students.

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 student based, within school or international.

4.4 We recognise that students need to understand how to style an e-mail in relation to their age and intended recipient.

4.5 See the separate Data Protection policy for further details and guidance.

5. Managing email

5.1 The academy gives all staff (and students) 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 students, parents or conduct any academy business using personal e-mail addresses. Staff should never use students' 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 student 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 Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

5.7 Staff must inform the eSafety coordinator if they receive an offensive e-mail.

5.8 Students 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 (i.e. anything classified as "Protect" or "Restricted" in accordance with the Data Protection policy). 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. If you need to send such information to another email domain, please check with the relevant IAO and contact IT Services for advice. Always check the recipient prior to sending.

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.

7. Receiving emails

7.1 Check your e-mail regularly.

7.2 Activate your 'out-of-office' notification when away for extended periods.

7.3 Never open attachments or click on links from an untrusted source.

7.4 If in doubt: delete.

8. eSafety Roles and responsibilities

8.1 Roles and Responsibilities

8.1.1 As eSafety 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 eSafety coordinator 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 eSafety 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 by the eSafety co-ordinator and all 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 students, is to protect the interests and safety of the whole community.

8.2 eSafety in the Curriculum

8.2.1 ICT and online resources are increasingly used across the curriculum. It is essential for eSafety guidance to be given to the students on a regular and meaningful basis.

8.2.2 eSafety is embedded within the curriculum and academies must continually look for new opportunities to promote eSafety.

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.

8.2.4 Educating students on the dangers of technologies that may be encountered outside the academy is done informally when opportunities arise and as part of the eSafety curriculum.

8.2.5 Students are taught about copyright and respecting other people's information, safe use of images, taking and recording of pictures and videos, etc through discussion, modelling and activities.

8.2.6 Students must be aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying. Students 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."

8.2.7 Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

8.3 E-Safety skills development for staff

8.3.1 Staff receive regular information and training on eSafety 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 eSafety 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 eSafety activities and awareness within their curriculum areas.

8.3.4 Endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.

8.3.5 The eSafety policy is introduced to the students at the start of each school year.

8.4 Incident reporting, eSafety 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 eSafety Co-ordinator. 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.

8.5 eSafety incident log

8.5.1 Any incidents will be recorded by the eSafety coordinator (administrative support available) in the eSafety log, stored securely in a documented location on the academy's network – the layout of which is presented below:

- Date & Time Name of student or staff member
- Gender Room and computer or device identifier
- Details of incident (including evidence)
- Actions and reasons

9 .Misuse and infringements

9.1 Complaints

9.1.1 Complaints and/ or issues relating to eSafety should be made to the eSafety 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 eSafety co-ordinator.

9.2.2 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Principal, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see below).

9.3 Managing an eSafety 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 students 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, students or others, or any other confidential information acquired through your job on any social networking site or other online system.

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 student is found to be accessing such material without legitimate purpose (e.g. as part of a Citizenship assignment), it should be treated as a safeguarding issue.

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 students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

15.2 Students:

15.2.1 All students 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 Students 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 Students 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 students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

15.2.5 Students are encouraged to be wary about publishing specific and detailed private thoughts online

15.2.6 Our students 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

15.2.7 In extreme cases, where a student feels threatened or at risk, the student should immediately contact the NCA's CEOP Command

15.2.8 Students must not use public social media for school business without the knowledge of the eSafety Coordinator. Students wishing to have a blog created for an approved school group, society, team or event may contact IT Services who will be happy to oblige or advise further.

15.3 Staff:

15.3.1 Staff may only create blogs, wikis or other online systems in order to communicate with students using systems approved by the eSafety Coordinator.

15.3.2 We do not permit any use of Facebook or other social media sites to engage with students for social purposes but may allow access to such sites by individual approval and agreement with the eSafety 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 eSafety coordinator must be informed of any blogs created or endorsed by members of staff for use with students. 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 MCMA.

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.

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 students must be declined.

15.3.12 Staff must not establish contact with students through their personal social networking sites, or any other means of electronic communication (including personal email or telephone). All contact with students must be directly concerned with the students' education.

15.3.13 We advise that staff refrain from contacting former students via personal email or social media.

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. Be aware that this may lead to indirect communication with students – 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 students 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.

16. Parental involvement

16.1 We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities.

16.2 We regularly consult and discuss eSafety 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 are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on academy website)

16.5 The academy disseminates information to parents relating to eSafety where appropriate in the form of eg Information evenings, leaflet drops, Website postings, Email or Twitter

17 Academy owned ICT equipment (also see data protection section)

17.1 As a user of IT, you are responsible for any activity undertaken on the academy's ICT equipment provided to you.

17.2 The academy logs IT equipment issued to staff and record serial numbers as part of the academy's asset register.

17.3 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.

17.4 A time locking screensaver is applied to all machines. Please lock your machine when you move away from it – even momentarily.

17.5 Privately owned ICT equipment may only be connected to the Wi-Fi network – contact your IT Services team for further guidance.

17.6 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.

17.7 All IT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:

17.7.1 Liaising with IT Services to ensure compatibility and to benefit from the Academy's purchasing schemes.

17.7.2 maintaining control of the allocation and transfer within their Unit.

17.7.3 recovering and returning equipment when no longer needed.

17.7.4 All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA) .

18. Portable and mobile ICT equipment

18.1 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.

18.2 All activities carried out on academy systems and hardware will be monitored in accordance with the general policy:

18.2.1 Ensure portable and mobile IT equipment is made available as necessary for antivirus updates and software installations, patches or upgrades.

18.2.2 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.

18.2.3 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.

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 students.

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 Data Protection Policy 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 Students are allowed to bring personal mobile devices/phones to the academy but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent unless specific teacher permission has been given. Personal phonecalls should not be made during the day.

20.1.2 This technology may be used, however for educational purposes, as mutually agreed with the eSafety 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 students) 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).

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)

.

25. Current legislation

25.1 Acts relating to monitoring of staff email and activity

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other acts relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to

engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain: ☐access to computer files or software without permission (for example using another persons password to access files) ☐unauthorised access, as above, in order to commit a further criminal act (such as fraud) ☐impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these

purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts relating to the protection of personal data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

The Counter-Terrorism and Security Act 2015:

http://www.legislation.gov.uk/ukpga/2015/6/contents/enacted

Specific guidance for schools can be found in sections 57-76 of the following document:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_R evised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

eSafety Coordinator Mr M Gilbert

eSafety link governor Safeguarding Governor

IT Services team Mark Greenhalgh and Peter Tymkiw

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

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

If staff or students 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.

Students 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."

Students 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 students 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)

Acceptable Use Agreement: Students - found in the student planner

Acceptable use agreement: Staff – found in the operational handbook

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. For further details see this quick reference guide produced by the Information Commissioner's Office. Note than any reference to the religion, or racial or ethnic origin of the individual is subject to stricter controls.

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.

SIRO Senior Information Risk Officer (see Data Protection Policy)