John Cabot Academy

E-Safety Policy

Date Adopted: Feb 2016 , John Cabot Academy
Implementation date: Approved Feb 2016

1 Introduction

1.1 John Cabot Academy will allow students, teachers and co professionals access to network services and the Internet. All network activity and Internet access in the Academy must be in support of education and or research and must be appropriate to the educational objective of the Academy. It is important that all network users are aware that systems are in place to track and record what is happening across the structured cabled network and wireless cloud. This policy applies to all members of the Academy community (including staff, students, volunteers, parents, visitors and community users) who have been granted a user account or access to the John Cabot Academy ICT systems, both in and out of Academy and by remote connection. Anyone who is aware of any type of E-Safety issue that is taking place is expected to tell a member of staff immediately. Students before and after school access their phones as they would at home due to the mobile phone ban throughout the school day.

2 Rationale

2.1 New technologies have become integral to the lives of children and young people in today's society both within the Academy and in their lives outside of school. The Internet and other digital and information technologies are powerful tools, which offer unimaginable opportunities, and is constantly evolving and opening up new opportunities for everyone. Access to the Internet is becoming universal and increasingly more mobile. Correct use of electronic communication helps teachers and students to learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

2.2 John Cabot Academy has a duty to provide students with adequate Internet access to allow our students to access resources enabling them to explore, enhance and develop their learning experience. Internet use is part of the statutory curriculum and a necessary tool for both staff and students.

2.3 Correct use of online resources is a necessary first order skill and one that we need to develop in our students so that they can become effective citizens and lifelong learners. The students and staff at John Cabot Academy should have an entitlement to safe internet access at all times; however, if misuse is an issue, steps to restrict or prevent access will be put in place to safeguard the individuals and network infrastructure.

3 Roles and Responsibilities

3.1 The Academy Principal is ultimately responsible for ensuring the safety of the students and staff at John Cabot Academy (including e-safety). The Academy Principal and the Senior Leadership team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff or student. It is important to remember that most of the incidents of e-safety or online use issues are completely unique and have to be dealt with sensitively and, depending on the incident, it may include a number of key staff and possible outside agencies.

3.2 The Academy Principal at John Cabot Academy has delegated the responsibility of e-safety security to a number of key staff within the ICT staffing structure. The Head of CLF ICT Operations and the assigned CLF ICT Operations Service Engineer to John Cabot Academy are responsible for the Academy's ICT infrastructure and it is their duty to ensure that it is secure and not open to misuse or malicious attack. All suspected misuse or problems must be reported to the E-Safety Coordinator and Academy Principal. The Academy's Safeguarding Lead and Safeguarding Councillor will be made aware of the potential for a serious safeguarding issue that could arise from the use of the Internet and other mobile handheld technologies connected to online resources. John Cabot Academy staff are aware that we all have a duty of care and should do our best to monitor the student's activity when we provided electronic devices or computer access in our learning and teaching activities.

4 Education – Students

4.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the Academy's e-safety provision. Children and young people need the help and support of the Academy to recognise and avoid e-safety risks and build their resilience.

4.2 The Academy implements an acceptable use policy for staff (Appendix 2) and students (Appendix 3).

4.3 E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing lessons and is regularly revisited.
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

5 Education & Training – Staff

5.1 It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy E-safety Policy and Acceptable Use Agreements.
- All staff will receive annual "refresher" training in e-safety as part of their annual safeguarding briefing.

6 Use of Digital and Video Images

6.1 The following principles apply to the use of digital and video images:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at Academy events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents comment on any activities involving other students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims but must follow Academy policies concerning the sharing, distribution and publication of those

images. Those images should only be taken on Academy equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names should not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents will be obtained before photographs of students are published on the Academy website as part of the Home School Agreement.

7 Social Media

7.1 Request a copy of the Social Media Policy for more information.

7.2 John Cabot Academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the Academy through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

7.3 Academy staff should ensure that:

- No reference should be made in personal social media to students, parents or Academy staff.
- They do not engage in online discussion with members of the Academy student community.
- Personal opinions should not be attributed to the Academy or Cabot Learning Federation.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

7.4 The Academy's use of social media for professional purposes will be checked regularly to ensure compliance with the Academy Social Media and Data Protection Policies.

8 Responding to Incidents of Misuse - Illegal Incidents

8.1 If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, the police will be informed.

9 Responding to Incidents of Misuse - Other Incidents

9.1 It is hoped that all members of the Academy community will be responsible users of digital technologies, who understand and follow Academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

9.2 In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures.
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action.
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour.
  - the sending of obscene materials to a child.
  - adult material which potentially breaches the Obscene Publications Act.
  - criminally racist material.
  - other criminal conduct, activity or materials.
  - Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

9.3 It is important that all of the above steps are taken as they will provide an evidence trail for the Academy, and possibly the police, and demonstrate that visits to these sites were carried out for safeguarding purposes.

Appendices

Can be found on the following pages:
- Appendix 1: Glossary of Terms
- Appendix 2: Staff Acceptable Use Policy
- Appendix 3: Student Acceptable Use Policy

Policy agreed by Academy Council: February 2015
Policy to be reviewed: February 2016

Appendix 1
Glossary of terms

AUP	An Acceptable Use Policy is a set of rules applied by the owner or manager of a network, website, service, or large computer system that defines the permissive ways in which the network, website or system may be used.
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes. See: http://ceop.police.uk/
CLF	Cabot Learning Federation. See: http://www.cabotlearningfederation.net/
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health & Wellbeing
ICO	Information Commissioners Officer. See: https://ico.org.uk/
ICT	Information & Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education & Training
IP address	The label that identifies each computer to other computers using the IP (Internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain
Ofcom	Office of Communications (independent communications sector regulator)
SC	Safeguarding Committee
SLT	Senior Leadership Team / Senior Management Team
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
Think U Know	An educational e-safety programme for schools, young people and parents
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting
WAP	Wireless Application Protocol

Appendix 2

Staff Acceptable Use Policy

The following is displayed upon logging on to the networked computer systems to all members of staff every 60 days or when the AUP has been changed:

The school has provided computers for use by staff, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Always get permission before installing, attempting to install or storing programs of any type on the computers.
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the ICT equipment.
- Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.
- Always check files brought in on removable media (such as floppy disks, CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
- Always check mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Always be wary about revealing your home address, telephone number, school name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Computer storage areas and floppy disks will be treated like school lockers. ICT staff may review your files and communications to ensure that you are using the system responsibly.

Internet

- You should access the Internet only for school activities.
- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- 'Chat' activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons 'chat' rooms should be avoided.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet will be denied and you will be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Appendix 3

Student Acceptable Use Policy

The following is displayed upon logging on to the networked computer systems to all students at JCA every 60 days or when the AUP has been changed:

JCA IT systems Acceptable Use Policy

This applies to everyone who uses IT equipment in JCA and includes all computer related activity that covers your login information, your files, email, learning environment and any computer system related to John Cabot Academy.

Users of the JCA IT systems must agree to:

- I will not use the JCA IT systems for communicating, uploading, storing, viewing or transmitting any material which is (or may be considered to be) defamatory, inflammatory, discriminatory, threatening, harassing, obscene or offensive. For example: insulting/bullying others, stirring others, racism, and sexism by e-mail, texting, posting online are not acceptable.
- I will not misrepresent the academy or bring it into disrepute in any way through the use of JCA IT systems. For example: taking videos/photos of the Academy's buildings and members and posting them online to something like YouTube or sharing them on Facebook where it is likely to cause embarrassment and harm.
- I will look after my own username and password. I will not share my password with anyone else and not use the username and password of other users.
- I will keep my computer secure. For example, I will not login to the IT systems and then leave my computer unattended.
- I will report all hardware and computer faults to staff and not attempt to fix equipment myself, including connecting and disconnecting it.
- I will make every attempt to ensure my work is free from viruses that may damage the IT systems. I will not use any files, or memory sticks that contains viruses or other programs which may disrupt the academy's systems.
- I will not attempt to gain unauthorised access to any part of the IT Systems that I do not have access to.
- I will not attempt to access, upload private, confidential or sensitive material unless this is authorised.
- I will not use any software, websites, or other means to access filtered sites. For example: using a proxy site to access a website that is usually filtered
- I will not use the IT systems for anything else other than for the purposes of teaching, learning and research.
- I will not use the IT systems for personal commercial use or use it for advertising, promotion or sale of commercial products or services without permission. I will ensure I will backup work and data regularly and sensibly.
- I will not breach the copyright of the academy or any third party by copying from the IT systems without authorisation. This includes the work of others without their permission and copying software without appropriate permission.

Enforcement
Breaches will be dealt with in line with the Academy's Sanctions Policy and could, in extreme cases, result in an individual being asked to leave the Academy.