INFORMATION TECHNOLOGY POLICY

The use of Information and Communications (ICT) at the Academy School is about learning. The educational and social benefits for children in using the internet should be balanced against the need to safeguard against the inherent risks from internet technology. The use of ICT brings with it new concerns about attitudes and values. It is our task to ensure that attitudes and values evolve to maximise students' opportunities to evolve into responsible citizens. This policy has been developed and implemented with due regard to Camden's "Model e-safety policy for schools and colleges in Camden", the Independent School Regulations 2014 and Keeping Children Safe in Education 2020.

Aims and scope of the Policy

This policy applies to all computers on the school premises that can connect to the internet or otherwise be used for data processing, referred to as "computers". This includes: -

- The voice and data networks that connect them
- All devices connected to these computers and networks
- The hardware and software associated with these systems
- The information managed by these systems

Each user is responsible for his/her actions whether or not rules are built in, and whether or not they can be circumvented. This means, for example, that even if a password becomes known or if a person has the technical ability to circumvent the password, that person still has the responsibility to other users and the school as owner of the computer system.

There are many ways in which the above principles can be breached. The following list of examples is not exclusive but may serve to give guidance within the school context: -

- Deliberately obtaining, possessing, using, or attempting to use passwords or other access information belonging to someone else
- Knowingly tampering with, obstructing, or impairing the availability of ICT resources
- Deliberately introducing damaging, self-propagating, or otherwise harmful software into a machine or a network
- Knowingly introducing unauthorised executable files and other applications
- Attempting to remove or modify computer or network equipment or software without proper authorisation

Risk

The risk associated with use of technology can be grouped into 4 categories: -

Content

Children may be exposed to inappropriate images such as pornography, or information advocating violence, racism, suicide or illegal and anti-social behaviour that they are unable to evaluate in a critical manner. Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent. The internet may also be used as a way of bullying a child, known as cyber bullying.

Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud.

Contact

Chat rooms, gaming sites and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as grooming) with a view to sexually abusing them.

Culture

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- Becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- Using information from the internet in a way that breaches copyright laws
- Uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience.
- Cyber bullying
- Use of mobile devices to take and distribute inappropriate images of the young person that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

Responsibilities

The ultimate responsibility for judgement as to what is or is not appropriate educational use lies with the Headmaster who is also the Designated Safeguarding Lead ("DSL"). This responsibility may be delegated to other members of staff. The school reserves the right for the Headmaster to access any student computer for the purposes of monitoring the appropriate use of the Internet, email and any other file or programme created or used whilst on the school's premises.

The Headmaster's responsibilities include: -

- The overall development and implementation of the school's e-safety
- Ensuring that e-safety issues are given a high profile within the school community
- Ensuring that e-safety is embedded in the curriculum
- Deciding on sanctions against staff and pupils who are in breach of acceptable use policies
- Developing, implementing, monitoring and reviewing the school's e-safety policy
- Maintaining a log of internet related incidents and co-ordinate any investigation into breaches
- Reporting all serious incidents and issues to Camden's e-safety officer.

The responsibilities of the staff of the Academy School include: -

- Adhering to the school's e-safety and acceptable use policy and procedures
- Communicating the school's e-safety and acceptable use policy to pupils
- Keeping pupils safe and ensuring they receive appropriate supervision and support whilst using the internet
- Reporting breaches of internet use, either by pupils or staff, to the headmaster
- Recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action

Child protection issues

Where any e-safety incident has serious implications for the child's safety or well-being, the matter should be referred to the Headmaster acting as DSL who will decide whether or not a referral should be made to Family Services and Social Work or the Police. The designated Person should be aware that pupils with learning difficulties or disability may be more vulnerable to risk from the use of the internet and may need additional guidance on e-safety practice as well as closer supervision.

Liaison with Parents

The school will maintain close contact with parents on e-safety issues and discuss any issues of concern as soon as they arise.

Accessing and monitoring the system

All internet access by children should be supervised by a member of staff. It is a duty of all members of staff to raise any concerns they may have regarding social media and information technology with the Designated Person. We have established filtering systems on our computers to ensure that inappropriate sites are not accessible. Pupils are only allowed to access the internet in supervised lessons where the computer they are using is recorded or under the direct supervision of a member of staff, again where the computer they are using is recorded.

Teaching e-safety

The school is committed to teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own

behaviour and internet use so that they can be given more freedom to explore systems with a lessening amount of supervision from staff.

Pupils are taught all elements of e-safety so that they

- Use technology safely and respectively, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems
- Are responsible, competent, confident and creative users of information and communication technology
- That they should understand that any material sent over the internet could be passed onto third parties

IT and safe teaching practice

Where staff need to communicate with pupils regarding school work, this should be via the school email system and messages should be carefully written to ensure that they are clear, unambiguous and not open to negative interpretation. Teachers should teach pupils good research skills that help them to maximise the resources available on the internet so that they can use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

Rules

The policy is based on the premise that access to the Internet is limited to acceptable educational purposes within the context of a lesson or as specifically authorised by a member of staff on school owned and operated computers, unless otherwise authorised by the Headmaster. Pupils shall never access inappropriate Internet sites even when access to banned sites and functions is not securely protected. Pupils shall never use their mobile phones during the school day. Mobile phones are solely to contact the pupil's parents or those looking after them before and after the school day. Computers of pupils may not be used to communicate in any way with friends, other family members or third parties whilst the pupil is on the school premises. Computers are not to be used to take, disseminate or receive photographs or to watch and/or listen to films or music. No gameboys or other forms of electronic devices are to be brought into the school.

Responding to incidents

All incidents and complaints relating to e-safety and unacceptable internet use should be reported to the Headmaster. All incidents, whether involving pupils or staff, must be recorded on the e-safety incident report form. If the incident is serious such that the safety of a child may be at risk, a copy of the incident record should be sent to Camden's designated e-safety officer jenni.spencer@camden.gov.uk. Where an incident relates to a member of staff, consideration should be given to contacting the LADO where this is appropriate. Incidents involving the Headmaster should be referred to Chair of Academy School (Hampstead) LLP. If materials viewed are illegal in nature the Headmaster should report the incident to the police and follow their advice

and this should be recorded on the incident form. A log of e-safety incidents and complaints should be maintained and reviewed for evidence of emerging patterns of individual behaviour or weaknesses in the school's e-safety system.

Cyberbullying

Cyberbullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows the distribution of hurtful comments and material to a wide audience.

Bullying may take the form of: -

- Rude, abusive or threatening messages via email or text
- Posting insulting, derogatory or defamatory statements on blogs or social networking sites
- Making or sharing derogatory or embarrassing images or videos of someone via mobile phone or email.

Incidents of cyberbullying are covered by the school's bullying policy but should also be recorded on an e-safety incident form. Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence. As part of e-safety awareness and education, pupils should be told of the "no tolerance" policy for cyber-bullying and encouraged to report incidents to their teacher.

Pupils are taught: -

- To only give out mobile phone numbers and email addresses to people they trust
- To only allow close friends whom they trust access to their social networking page
- Not to send or post inappropriate images of themselves
- Not to respond to offensive messages
- To report the matter to their parents and teacher immediately

Teachers may become victims of cyberbullying by pupils. Teachers can report any such incidents in confidence. Incidents of cyberbullying of teachers should be recorded on the e-safety incident forms.

Risk of contact from violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences. Staff need to be aware of those pupils who are being targeted by or exposed to harmful influences from violent extremists via the internet. Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies. All incidents involving violent extremism should be reviewed to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.

Sanctions

Action taken in response to serious or repeated violations of any part of the policy by pupils will be decided by the Headmaster. In serious cases this may result in suspension or expulsion. The school may restrict or terminate any student's access to its computers and internet, without prior notice, if such action is deemed necessary. If any of the above guidelines are breached the School reserves the right to inform the appropriate authorities. In relation to staff, any breach of this policy will be treated as a disciplinary matter and, in very serious cases, may result in dismissal for gross misconduct.

Reviewed and updated by Andrew Sandars

July 2020