E-Safety Policy

(May 2015)

This Academy provides technology for use by all its stakeholders**.** They offer access to a vast range of valuable information for use in education and are an enormous extension to the information base held in the Academy Learning Resource Centre that will help users prepare for life in today's world.

The technologies are provided and maintained for the benefit of all users. Users are encouraged to use and enjoy these resources and we wish to ensure that they remain available to all. To protect all in its care, the Academy must insist that all users adhere to these rules for acceptable use of the technologies.

The Academy reserves the right to examine or delete any files that may be held on its network and to monitor the network including Internet sites visited and emails sent.

Due to the nature of some educational courses some rules may not be appropriate at certain points in the curriculum as they form part of the course content). In these special cases the teacher will give specific permission.

The Academy will deliver annual "e-safety and internet awareness" assemblies from the CEOP website Think U Know. This will be delivered to all year groups. In addition, Year 7 students will be taught with an introductory scheme of work on e-safety. This will be followed up in Year 8 when students will have the opportunity to follow a scheme of work about cyber security.

Definitions:

Technology = PC's, printers, external devices, mobile phones, PDA's, Tablets, USB pens, Bluetooth, mp3 etc

Users = anyone who uses the resources (pupils, staff, parents, Directors, community etc)

Exchange information = any technology device used e.g. Internet, email, Bluetooth, USB pens etc

Rules:

1. All Internet use should be for educational purposes.

2. Users may not install or attempt to install programs of any type on a machine, or store programs on the computers unless authorised by the IT Manager

3. Users must not damage, disable, steal or otherwise harm the operation of equipment, or intentionally waste limited resources.

4. Users will not use the network for commercial purposes, personal financial gain or gambling.

5. Users must not disclose their passwords to others or attempt to logon to another user's account.

6. Users making use of the technologies must do so in a way that does not harm, harass, offend or insult others. Appropriate language must be used at all times.

7. Users are expected to respect and not attempt to bypass or alter security settings. This includes the use of proxy servers.

8. Users must not access, copy, remove or otherwise alter other users' work. Staff may access students work for assessment and moderation purposes.

9. Users must not alter computer settings.

10. Users may use personal external devices such as mobile phones, tablets, PDA's, USB devices, mp3, mp4 etc when planned for educational purposes and their teacher gives permission. Inappropriate use will result in equipment being confiscated in line with Academy policy.

11. Any faults with any equipment MUST be reported to the teacher and users should make no attempt at repairs.

12. Users must not disclose or share personal information of themselves or others on-line.

13. Activity that threatens the integrity of the Academy ICT systems, or that attacks or corrupts other systems, is forbidden.

14. Users must not engage in for example chat/social networking/IM activities over the Internet unless authorised to do so by a teacher. This takes up valuable resources which could be used by others to benefit their studies and can lead to unwelcome material being brought into the Academy.

15. Users must not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are inappropriate, unlawful, or that may cause harm or distress to others.

16. Users are responsible for exchanging information via digital communication and therefore the same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.

17. Posting anonymous messages and forwarding chain letters is forbidden.

18. Users are expected to respect the work and ownership rights of people both inside and outside the Academy. This includes abiding by laws relating to technologies e.g. copyright laws.

19. All students/parents or carers read and sign an 'ICT Acceptable User Statement' which is kept on their file. See ICT Acceptable Use Policy.

Behaviours

These behaviours will link in with the behaviour policy sanctions as part of the whole Academy policy. All incidents will be dealt with individually following Academy protocols.

Level 1

- Food and drink consumed in ICT suites.
- Off task behaviours e.g. websites, games etc.
- Downloading without permission
- Inappropriate/excessive printing
- Inappropriate use of external devices e.g. USB, mp3, mp4, mobile phones etc.

Level 1 sanctions may include temporary loss of access to network, e-mail and internet, detentions, informing parents where applicable and internal exclusions. The classroom teacher must liaise with the HOF after statements have been taken and signed by student(s) involved in order to determine which sanction is appropriate. All incidents and actions taken must be recorded on SIMS. HOF will contact parents

Level 2

- Minor damage to equipment
- Abusing others work
- Sharing passwords
- Inappropriate use of language
- Inappropriate use of internet
- Inappropriate use of e-mail
- Inappropriate use of text, images, sound, video and other media

Level 2 sanctions may include temporary loss of access to network, e-mail and internet, internal exclusions, informing parents where applicable and or sessions in the CIC. The classroom teacher works in conjunction with the HOF after statements have been taken and signed from student(s) involved. The HOF then contacts SWi/IS in order to determine which sanction is the most appropriate. All incidents and actions taken must be recorded on SIMS. HOF or HOY will contact parents.

Level 3

- Hacking
- Logging on as another user
- Bypassing security settings
- Using proxy sites
- Major damage to equipment
- Cyber bullying
- Unauthorised access
- Disconnecting cables, devices etc. or changing settings

Level 3 sanctions may include temporary loss of access to network, e-mail and internet, informing parents, internal exclusion, sessions in the CIC and/or fixed-term exclusion and in some instances may lead to permanent exclusion. The classroom teacher works in conjunction with the HOF who then contacts SWi/IS in order to determine which sanction is the most appropriate after statements have been taken and signed from student(s) involved. All incidents and actions taken must be recorded on SIMS. Main investigating member of staff to contact parents.

Level 4

- Illegal activity: this will be dealt with by the Principal and external agencies in line with the law.

Level 4 sanctions will include temporary/permanent loss of access to network, e-mail and internet, fixed-term exclusion and in some instances may lead to permanent exclusion.

Legislation relating to Technologies:

The user must comply with all relevant legislation and legal precedent, including the provisions of the following Acts of Parliament, or any re-enactment thereof:

- **Copyright, Designs and Patents Act 1988**;
- **Malicious Communications Act 1988**;
- **Computer Misuse Act 1990**;
- **Criminal Justice and Public Order Act 1994**;
- **Trade Marks Act 1994**
- **Electronic Communications Act 2000**

- **Data Protection Act 1998**;
- **Human Rights Act 1998**;
- **Regulation of Investigatory Powers Act 2000**;
- **Freedom of Information Act 2000**;
- **Communications Act 2003**.

See below for a summary of the main points.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. you tube).

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the Academy context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The Academy reserves the right to monitor its systems and communications in line with its rights under this act.

The e-safety policy should be read in conjunction with other relevant policies:

- Communications
- Behaviour for Learning
- Child Protection
- Anti-bullying
- Mobile phone
- ICT Acceptable Use Policy

Policy adopted from Churchfields Academy on 1st September 2017
Updated Date: March 2015
Person Responsible: Vice Principal and Head of Creative Technologies
Approved by the Governing Board Achievement committee: May 2015
Review Date: May 2018