County High School, Leftwich

Acceptable Use Policy

Purpose

The purpose of this policy is to:

- ensure that the academy complies with all laws and regulations regarding the storage, use, dissemination and transmission of information (see separate 'Legal Basis' document for details);
- ensure that the academy's ICT systems are adequately protected against misuse or abuse; and
- ensure that users are aware of, and agree to be bound by, certain responsibilities in their use of the academy's ICT systems.

Scope

The academy's ICT systems are provided to staff and students to enable them to better carry out their teaching and learning respectively. For the purposes of this document, 'ICT systems' includes, but is not limited to:

- all hardware devices on the academy site, whether owned by the academy or not;
- all software programs, including all physical media (CD's, disks *etc.*) on site, whether owned by the academy or not, and any electronic implementation thereof;
- all web-based resources including email whether located externally (and accessed from within the academy) or internally (and accessed from either within or beyond the academy),
- the academy's MIS system (Capita SIMS) and
- all network services, wired and wireless.

Acceptable Use Contract

The academy requires all authorised users of the academy's ICT systems to consent to be bound by this policy. Unauthorised use of the systems or use that is contrary to this policy will result in the relevant disciplinary procedure being followed. This could result ultimately in exclusion of students or dismissal of staff. In the event of a serious infringement the academy may also decide to institute legal proceedings under the relevant civil or criminal law (see separate 'Legal Basis' document for details).

Further information relating to acceptable use is available in the academy's Online, Data Protection and Child Protection Policies.

Responsibilities of Users

Physical Devices

Users must take appropriate care of the physical devices owned by the academy and loaned to or used by them. The academy will review the access granted to such devices in the event that such appropriate care is not taken.

Security

Authorised ICT system users are allocated usernames and passwords to control access to systems. Users' responsibilities in respect of such security are as follows.

- The user is responsible for the confidentiality of the username and password and must take steps to change their password if they believe it has become known to others.

- Users must respect any password policies in place from time to time and communicated via the Director of Finance responsible for ICT infrastructure or the IT Technician.
- Users must not use anyone else's username/password without that user's permission.
- Users must not obtain or try to obtain anyone else's password without their permission.
- Users must inform the IT Technician immediately if they suspect someone else of using another person's username/password.
- Teachers must not leave computers unattended when logged in unless they have 'locked' the computer in such a way that their password is required for access.

Computer Network and Networked Resources

Users must not connect any device to the network, or to a computer connected to the network, without the permission of the IT Technician.

With the exception of the Senior Leadership Team and IT Technician, users must not gain access or attempt to gain access to any files owned by someone else unless the owner has specifically granted such access. This does not apply to teachers gaining access to student areas in the course of their academic duties.

Users must not knowingly introduce malicious code including viruses, network worms, Trojan horses, logic bombs etc and must be mindful at all times of the risk of introducing such code through removable media (such as 'pen' drives or memory sticks) and through email attachments.

Users must not install software on academy equipment without permission from the IT Technician or Director of Finance responsible for ICT infrastructure.

Users are entirely responsible for the contents of their email, 'home directory', e-portfolio or other area designated for their sole use. The academy may delete these areas in their entirety following the cessation of employment or enrolment as a student.

Unacceptable use of technology

- Verbal, written or electronically transmitted abuse of any person including indecent or obscene expressions of conduct or threat of physical abuse to any person.
- Verbal, written or electronically transmitted harassment: defined as behaviour directed at a member of the academy community which would cause emotional distress, intimidation, or coercion to a reasonable person in the victim's position.
- Failure to respect the privacy of other individuals through the use of technology.
- Use by an adult for personal reasons is acceptable except where the activity might reasonably be considered to be contrary to the ethos of the academy or bring the academy into disrepute.
- Failure by a student to follow the instructions of their teacher or other responsible adult within the academy concerning their use of ICT particularly in respect of the information which they are allowed to access, the applications they are allowed to use and the resources they are allowed to consume.
- Installation of any unauthorised software.
- Storage of non-business related software or documents.
- Any tampering (e.g setting a BIOS password, removing casing etc).
- Leaving PCs unattended and logged in for extended periods.
- Use of unapproved screensavers and backdrops.
- Hacking or snooping (e.g attempting to gain access to areas/systems known to be unauthorised.

- Unauthorised connection of equipment to any part of the Academy network – in particular laptop computers.
- Accessing sites that contain defamatory, obscene/pornographic text, messages or images.

Academic Dishonesty/Cheating

Users must not use ICT systems to cheat in academic assessments. The relevant forms of cheating include the following.

- Unauthorised assistance: communication to another through electronic means.
- The unauthorised possession or use of examination or course related material.
- Plagiarism: whereby another's work is deliberately used or appropriated without any indication of the source, thereby attempting to convey the impression that such work is the student's own.
- Any person who knowingly helps someone else to cheat.

Responsibilities of System Administrators

The IT Technician and other users with 'systems administration' rights have the same responsibilities as other users, plus additional responsibilities and privileges due to their administrative position. An external IT support provider is retained to proactively monitor the ICT systems and support the IT Technician to maintain them. Someone with these rights:

- is responsible for establishing appropriate user privileges and monitoring access for the systems they administer;
- is expected to take reasonable precautions to safeguard against corruption, compromise or destruction of data, computer systems, and network resources;
- is expected to maintain the ICT systems in a way that minimises the chance of unauthorised access;
- is expected to ensure that systems security patches, upgrades and software (such as spam filters and anti-virus software) are kept up to date where possible and such that the service is not adversely affected;
- must ensure within reason that all software in use is properly licensed; and
- must ensure adequate backup and disaster recovery procedures are in place, monitored and tested for effectiveness.

Confidentiality, Privacy and Internet Safety

Users have a duty of care to protect the confidentiality of any information that they might access though the academy ICT systems in the course of legitimate employment activities or through academic studies.

The academy reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the academy and no user shall have any expectation of privacy regarding such materials.

Always be mindful that people you 'meet' on the Internet may not be who they say they are: never reveal personal details such as addresses, student names, or photographs.

County High School, Leftwich

Acceptable Use and Online Policies – Legal Basis

Laws Covering Hacking, Privacy and Protection of Personal Data

Computer Misuse Act (1990)

This Act creates three criminal offences.

1. Unauthorised access to computer material

This makes it illegal to access a computing system unless authorised to do so. As such it makes the activity of "hacking" a crime. It does not matter whether the hacker is remote, working from a distance over the remote area networks, or local, where persons such as employees or students who may have limited authorisation to use the computers but they knowingly exceed that authority. The hacking need not be directed at a particular computer, program or data. For example, it is unlawful, without proper authority:

- to use another person's ID and password in order to access a computer, use data or run a program;
- to alter, delete, copy, or move a program or data, or simply to output a program or data; or
- to lay a trap to obtain a password.

2. Unauthorised access to a computer system with intent to commit or facilitate the commission of a further offence

This covers the situation where unauthorised access is gained with intent to commit a further offence. For example, a person may gain unauthorised access to a computer via another person's ID in order to transmit offensive material or access confidential material.

3. Unauthorised modification of computer material

This offence includes the deliberate deletion or corruption of programs or data. It also includes the introduction of viruses etc, where these result in the modification or destruction of data.

The first of these three offences would most likely be dealt with in a magistrates' court, but the other two are considered to be serious and would be referred to the Crown court where very large fines and/or jail sentences are possible.

General data Protection Regulations (2018)

This Act requires that all data relating to other living persons, with the exception of personal data held by an individual for domestic or recreational purposes, should not be stored or processed on a computer system or in a relevant manual file by any person unless the purpose for which that data is stored is registered. Once the purpose is registered it will normally require the consent of the person concerned to use the data for another purpose. Such personal data includes that contained in photographs, videos and CCTV film which would enable a person to be identified.

Central to the Act are the six Principles which require personal data to be fairly processed, processed only for such purposes for which it is registered, is kept to a minimum for that purpose, kept accurate and up to date and only for such time as is necessary to achieve that purpose and is kept securely. The principles also provide

for individuals to obtain details of the data held about themselves and, where appropriate, to have data corrected or deleted.

The academy will not publish images of students in which the student can be identified by name and in any case not at all if such permission has been explicitly refused by parents.

Copyright, Designs and Patents Act (1988)

Under this Act it is unlawful to take an unauthorised copy of someone else's work. A person holds the copyright in that work if it is the product of their intellectual activity and hence is their intellectual property, although if that work is done as part of your employment the intellectual property and hence the copyright, is owned by the academy. Do not use someone else's work unless:-

- you have that person's permission; or
- you are sure that the material is in the Public Domain; or
- you are sure that the material is not protected by copyright.

Usage includes storing and displaying material electronically.

Laws Covering Offences of a Sexual Nature

The Internet is becoming more accessible to minors through computers in homes and schools. Material must not be published which might lead to injury or damage to minors. This includes material which is pornographic or excessively violent. You should be aware that some legitimate research documents may include material of a medical nature which is unsuitable for minors who must, therefore, be protected from unauthorised viewing.

The retention or display of pornographic or sexually-explicit material is forbidden by the academy, as is the enablement of links to sites containing such material. This is irrespective of whether that material is legal in this country or any other. The Criminal Justice and Public Order Act 1994 broadens the scope of the Obscene Publications Act 1959 making the storage and electronic transmission of pornographic material arrestable offences.

Sexual Offences Act 2003

<u>Grooming</u>
If you are over 18 and have communicated with a child under 16 at least twice (including by phone or 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.

<u>Making indecent images</u>
It is an offence to take, make, distribute, show, advertise indecent images of a child under 18. (NB even to *view* an indecent image on your computer means that you have made a digital image.)

<u>Causing a child under 16 to watch a Sexual Act</u>
To intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.

<u>Abuse of positions of trust</u>
Staff need to be aware that it is 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. (Applies to teachers, social workers, health professionals, Connexions PA's etc.)

Laws Covering Discrimination and Cyberbullying

Any material which bullies, harasses, discriminates or encourages discrimination on the grounds of age, disability, gender reassignment, race (including colour, nationality, ethnic or national origins), religion or belief, sex orientation or otherwise is in contravention of the Equality Act 2010.

Libel

Facts which concern individuals or organisations must be accurate and verifiable. Views or opinions must not portray their subjects in any way which would damage their reputation.

Public Order Act (1986)

It is an offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

Telecommunications Act (1984)

It is an offence to send by public telecommunications network any offensive, indecent, obscene or menacing messages that cause annoyance / inconvenience / needless anxiety.

Malicious Communications Act (1988)

It is an offence to send a letter or article which includes indecent, grossly offensive, threatening or false information with the intent of causing anxiety/stress to the recipient.

Protection from Harassment Act (1997)

Section 1 - 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.

Section 4 - 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.

Incitement

Users must not publish anything which might incite others to commit criminal acts or even to contemplate them.

Approved by Governors at Resources Committee: 12th November 2019
Ratified at Full Governors Meeting: 25th November 2019

Review Date: Autumn 2020

This document is part of the group which include Safeguarding, Child Protection, Behaviour for Learning, Anti-Bullying, E-Safety, Exclusions, Policy Statement Additional & Special Education Needs, Drugs' Education, Use of Images, Student Illness, Accident & First Aid, Use of Force, Recruitment, Single Equality Scheme and Health & Safety Policies.