CHESLYN HAY SPORT AND COMMUNITY HIGH SCHOOL

MANAGEMENT POLICY

Information and Communication Technology Security (Summary Version)

Introduction

For our school to be effective not only do we need to have ICT systems that are reliable, accessible and rapid, we must also ensure that the systems are secure. This policy is designed to help us create a safe environment for the staff and students by clearly stating what is acceptable when using the school's ICT equipment and all the resources it provides. This policy applies to all staff members who use, or has access to, any of the school's ICT infrastructure and the data it may contain. As employees of the school all staff are expected to familiarise themselves with the content of this policy and its appendices and to adhere to the expectations at all times.

Objectives

The objectives of the Policy, which is intended for all school staff, including governors , who use or support the school's ICT systems or data, are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff understands the need for information and ICT security and their own responsibilities in this respect.

The integrity of the school network depends on the security policy implemented by each connected school. In addition to the ICT Security Policy there is also the E-Safety Policy which complements this policy and is available from the ICT Development Manager.

"Information" covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

The school's ICT Development Manager is responsible for the school's ICT equipment, systems and data with direct control over these assets and their use, including responsibility for access control and protection. The ICT Development Manager will be the official point of contact for ICT or information security issues.

Responsibilities

- Users of the school's ICT systems and data must comply with the requirements of the ICT Security Policy
- Users are responsible for notifying the ICT Support Department of any suspected or actual breach of ICT security. In the absence of the ICT Development Manager, users should report any such breach directly to the Director of Business and Finance or their SLT Line Manager.
- Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984 and any other related Acts that are available from the DFE.
- Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
- Adequate procedures must be established in respect of the ICT security implications of personnel changes.

Physical Security

- As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.
- Server rooms must be kept locked when unattended.
- Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
- All school owned ICT equipment and software should be recorded and an inventory maintained.
- Uninterruptible Power Supply (UPS) units are recommended for servers and network cabinets.
- Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.
- Equipment should be sited to avoid environmental damage.

- Do not leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.
- Do not give out sensitive information unless the recipient is authorised to receive it.
- Do not send sensitive/personal information via e-mail or post without suitable security measures being applied.
- Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.

System Security

- Users must not make, distribute or use unlicensed software or data.
- Users must not make or send threatening, offensive or harassing messages.
- Users must not create, possess or distribute obscene material.
- Users must ensure they have authorisation for private use of the school's computer facilities.
- The ICT Development Manager will determine the level of password control.
- Passwords should be memorised. If passwords must be written down they should be kept in a secure location.
- Passwords should not be revealed to unauthorised persons.
- Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data.
- Passwords should be changed at least termly.
- Passwords must be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.
- Regular backups of data, in accordance with the recommended backup strategy, must be maintained.
- Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.
- Security copies should be clearly marked and stored in a fireproof location and/or off site.

Virus Protection

- The ICT Support Department will ensure current and up to date anti-virus software is applied to all school ICT systems.
- Laptop users must ensure they update their virus protection at least weekly.
- The ICT Support Department will ensure operating systems are updated with critical security patches as soon as these are available.
- The ICT Support Department Manager will ensure users of home/school laptops check for critical security patches/Anti-virus updates when connecting laptops to the school BYOD network.
- Any suspected or actual virus infection must be reported immediately to the ICT Support Department.

Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so; because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Monitoring

To ensure the security of the network and prevention of harm to any individual or item of equipment it is understood that the school exercises its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites and emails and the deletion of inappropriate material.
No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. Additional monitoring is provided via the approved monitoring solution called E-Safe for Education. This is used to help support and monitor e-safety issues as required.

Disposal and Repair of Equipment

- The ICT Support Department must ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.
- It is important to ensure that any software remaining on a PC being relinquished is legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.
- The ICT Support Department must ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.
- The school will ensure that third parties are registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

Security Incidents

All suspected or actual breaches of the ICT security, including detection of computer viruses, must be reported to the ICT Development Manager, Director of Business and Finance or SLT Line Manager in their absence, who should report the incident to the SLA Provision Support Company which is currently Entrust Education Support Services (0300 111 8030).

Legislation

There are currently four separate legislative acts which the school is responsible for enforcing when any member of staff or students is using any of its ICT equipment:

- the Data Protection Acts 1984 & 1998
- the Computer Misuse Act 1990
- the Copyright, Designs and Patents Act 1988
- the Telecommunications Act 1984.

These different legislative acts are considered individually in Appendix A. It is the responsibility of all staff to read Appendix A carefully as any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

Implementation of Legislation

It is impossible to list and define every single aspect of the use of ICT in the school. It is down to the individual's common sense to apply this policy to all aspects of the day-to-day use of data and the ICT equipment in the school. To aid individuals in adopting best practice, staff are expected to act upon the following information.

Useful Terms

In the policy and its accompanying appendices certain terms are used as defined in the main by the Data Protection Act. A glossary can be found in Appendix B.

Acceptable Use Policies

When Staff and students join the school they are asked to sign to agree that they will use the network and internet responsibility. Formal copies of these agreements can be found in the full ICT Security Policy and E-Safety Policy which are available from the ICT Development Manager.

The above is an overview of the main sections of the ICT Security Policy. For a full copy of the detailed ICT Technical Security Policy and the E-Safety Policy these are available from the ICT Support Departmental Manager upon request.

Lead SLT member: PGR
Date of next review: summer term 2017
Reference: ICT Security Policy PGR 08 16

Appendix A

CHESLYN HAY SPORT AND COMMUNITY HIGH SCHOOL

MANAGEMENT POLICY

Information and Communication Technology - Legislation

There are currently four separate legislative acts which the school is responsible for enforcing when any member of its community is using any of its ICT equipment: the Data Protection Acts 1984 & 1998; Computer Misuse Act 1990; Copyright, Designs and Patents Act 1988; and the Telecommunications Act 1984. Any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

Data Protection Acts 1984 & 1998

The Data Protection Act was introduced to regulate the use of personal information about living individuals stored by organisations in electronic form and to enforce a responsible use of this data. An update to this now covers certain manual methods of storage. The Data Protection Act has eight principles.

1. Data must be collected and used fairly.
2. It must only be used and held for the reasons given to the Information Commissioner.
3. You cannot sell it or give it away unless stated as such to begin with.
4. It must be relevant to the purpose stated in the register.
5. It must be accurate and kept up-to-date.
6. It must be kept for as long as necessary and not indefinitely.
7. The information must be kept safe and secure. This includes keeping the information backed up and away from unauthorised access. It must not be left to be viewable by unauthorised access.
8. The files must not be transferred outside of the EU unless the receiving country has a suitable Data Protection law.

There are a couple of partial exemptions that can apply to a school environment.

1. A student has no right of access to personal files or to exam results before publication.
2. A data controller can keep information for any length of time if it is being used for statistical, historical or for research purposes.

Computer Misuse Act 1990

The Computer Misuse Act was passed to deal with the growing concern of computer system hacking and it made it a standalone offence. To begin with the act of hacking a system was considered a simple annoyance and was treated as mischievous behaviour. It did not take long, however, for this offence to be considered more severe as data was stolen or lost and whole systems could be rendered inoperable within minutes and without the owners of these systems knowing. The act introduced three new offences if they are undertaken intentionally (it is the intentional aspect that makes the offence applicable).

1. Unauthorised access to a computer system or data stored within.
2. Unauthorised access with intent to commit further criminal acts.
3. Unauthorised modification of computer data or systems.

An offence can range from simply looking at someone else's electronic data without permission (eg by finding or guessing someone else's password) to hacking into a bank's computer with the intent of changing bank account details to actually changing those details. Any of these offences carry either a minimum of a six month prison sentence and a maximum of five years and/or a fine.

Copyright, Designs & Patents Act 1988

This Act was introduced to protect the intellectual property of an individual or organisation and covers literacy, dramatic, musical, and artistic works. Computer programs and data are covered under "literacy" works. Where data and programs are obtained from an external individual or organisation, they remain their property and normally only under license or contract, may be used by another individual or organisation. Where these formal agreements have been reached the end user of the data or program must obey the terms of that agreement. Any copying or using of these programs or data where the intellectual right of the creator has been breached or unheeded is a serious and criminal act.

The Telecommunications Act 1984

The Telecommunications Act, amongst other things, makes it an offence to send "by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character".

Appendix B

CHESLYN HAY SPORT AND COMMUNITY HIGH SCHOOL

MANAGEMENT POLICY

Information and Communication Technology - Useful Terms

In the policy and its accompanying appendices certain terms are used as defined in the main by the Data Protection Act.

Data
Any information stored in an electronic or paper format concerning an individual.

Data Controller
A nominated person in an organisation who applies to the data commissioner for permission to store and use personal data.

Data User
Any member of staff who as part of their role in the school works with data.

Data Subject
A particular person whom has personal data stored about them somewhere within the school campus.

ICT Room
Any room which has an item of ICT equipment, either a full suite of computers or a single whiteboard workstation.

Workstation
A hierarchical term used to describe the common components that make up a computer that includes: monitor (CRT & TFT), base unit, mouse, keyboard, power cables and network cables.

Whiteboard system
A hierarchical term used to describe the components of a whiteboard system that includes: the workstation used to power the whiteboard, the whiteboard, projector, amplifier, speakers and whiteboard pens.

School Community all staff, students and guests who might use any of the ICT equipment within the school.