



Crofton School

STAFF ICT POLICY AND GUIDANCE

Objectives and rationale

We want to make the fullest use of new technology and the improvements it can offer to learning, teaching and administration.

We understand that the pace of change is very great and so we need to be flexible in our approach. We also recognise that students will very often know more than staff - this fact offers both opportunities and risks.

New technology in general (and the internet in particular) provides an invaluable resource which can really enhance students' learning; it may also place students and staff at risk and so its use needs to be subject to clear rules and procedures.

Strategies for implementation

This is a vital principle: if staff are in any doubt about expectations regarding their use of ICT, they **MUST ASK**. Similarly, if staff are worried about inappropriate material that might have been accessed by a student or might have found its way onto the network or their laptop they **MUST ASK** the Network Manager or their linked member of SLT about it.

Our responsibility to students

All school staff share a responsibility to keep students safe. In the context of ICT, this responsibility is discharged by:

- Modelling good practice
- Teaching them about good practice, especially as regards internet safety

- Monitoring students' use of new technologies and restricting their access to some parts of the web

Internet and E-mail Use

Staff should make use of email to communicate with other staff in preference to paper. Staff may communicate with students via email but only via their school email addresses - on no account should staff tell students their personal email contact details. Staff must be certain that email communication with students focuses exclusively on academic issues and that there is no possibility of misunderstanding or misinterpretation - if you are in any doubt about the appropriateness of email content, YOU MUST ASK.

Similarly, staff may communicate with parents via email. Staff must be aware that emails have the same legal status as letters and so they must seek SLT authorisation before sending them.

Software should not be downloaded from the Internet without prior agreement from either the Network Manager to ensure that we obtain appropriate licensing and so that software can be evaluated in relation to security risks.

Staff must monitor students' use of the internet and ensure that they do not access inappropriate material or have unauthorised contact with other web-users. Any violations or concerns must be reported to the Network Manager as soon as possible so that action can be taken to prevent further breaches. Staff should not use school computers to access the internet other than for professional purposes.

Staff laptops

Laptops are issued to all teaching and some support staff. The issued laptop remains school property and should only be used by its designated keeper for school-related tasks.

None of us has any right to privacy as far as the content of our school laptops is concerned and so it is absolutely essential that they are NEVER used for purposes inconsistent with the professional standards of school teachers.

The school has a range of security and monitoring software that will automatically detect inappropriate material. The school reserves the right, at any time, to inspect the inner workings of all school laptops, including records of internet sites visited, emails and attachments and any material downloaded. Using any school computer inappropriately can be a disciplinary offence.

Staff should treat laptops as they would any other valuable items and ensure that appropriate security measures are taken. Laptops should not be left unattended at school or in vehicles and care should be taken to ensure that any sensitive data is kept secure. It is imperative that laptops are locked by the user, if they have to leave it unattended even for short periods. It is the responsibility of the member of staff to whom it has been allocated to take all reasonable steps to prevent unauthorised access to the laptop.

Staff should not add software to their laptop. Software must not be copied from the laptop to another device. The Network Manager will carry out upgrades to software as required. Staff wishing to use subject specific software must liaise with the Network Manager to ensure that appropriate licences are held. Software will not be installed unless the school holds the appropriate licence.

Staff will be asked to sign for laptops and should be aware that this equipment will be audited at regular intervals, in accordance with HCC Policy and on return to ensure that equipment has been used within the guidelines specified. Where possible temporary laptops will be issued to cover auditing / updating and the most widely used programmes will be installed.

The School Network

Staff must ensure that any material they place or create on the network is appropriate. Network usage is monitored and inappropriate usage, including messaging, will be reported.

Staff should avoid storing large files (especially media files) on the network as far as possible. These cause the system to slow and restrict the capacity of the server.

Staff in leadership positions should oversee regular reviews of material held in their areas of the network and delete obsolete and duplicate material. ICT support staff are available to help and give advice on this.

Passwords

Passwords must be obscure: it is very good practice to include numbers and varied capitalisation; it is very bad practice to choose words that are easily associated with the member of staff in question and therefore guessable. HCC security advice now states that the following is recommended format for passwords:

- Be at least 7 characters long:
- Capital letters (A - Z)
- Lower case letters (a-z)
- Numbers (0-9)
- Non alpha-numeric characters (e.g. !, ", %, ^, [, })

Numbers 1, 3 5, 9, & 0 can be used to replace i, e, s, g & o respectively.

Passwords must not be divulged to others nor should they be kept in a place that someone could find them.

If staff suspect their password has been compromised, they must inform the Network Manager immediately so that a replacement can be issued and appropriate action taken.

Copyright

All software must be used in accordance with the terms of the licence. Making copies is often forbidden; where copying is forbidden, doing so is a criminal offence. Similarly, software for 'single use' must not be installed on more than one machine.

Staff must not install software on school machines, including those on departmental inventory or available on the web. They should liaise with the Network Manager who will then ensure that the appropriate licensing is held prior to organising the installation of software.

Staff need to be aware that unauthorised resources stored on the network include music and some video. These are subject to copyright as well, unless they are specifically royalty free or have a no copyright disclaimer on them. Copyright material anywhere on the server will be deleted by the network Manager without prior notice.

Advice may be sought from the Senior Leader responsible pertaining to copyright. Alternatively more information relating to this can be found at <http://www.intellectual-property.gov.uk>.

Misuse

It is forbidden, and may be a criminal offence, to:

- Gain unauthorised access to computer material or system.
- Gain unauthorised access with intent to commit or facilitate commission of further offences.
- Make unauthorised modification of computer material.
- Download copyrighted materials.

Staff need to ensure that students adhere to the Student ICT Agreement when using ICT equipment in school. Faculty and Subject Leaders are to ensure that copies of this are displayed in all areas with access to computer equipment and that students are reminded of appropriate use when necessary. In the event of a serious breach of the agreement by a student, staff should refer the matter to the Senior Leader responsible.

Data Protection

All personal data must be protected against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage.

The managers and team leaders responsible for computers within school must take steps to protect the security of personal information, eg do not declare passwords to others, do not leave personal data on public areas of machines and do not leave machines unattended once a log on has been made.

Use of Data Off Site

Staff intending to use data electronically outside of school need to be aware of and agree to the following guidelines.

- Understand that the school and subsequently the staff are bound to observe the Data Protection Act. Staff must ensure that data is used/processed lawfully ie that the use to which it is put is specified and lawful and that data is not disclosed in any manner incompatible with that specified use. Data should not be not held for any longer than is necessary and appropriate measures must be taken against

unauthorised access, alteration, disclosure or accidental loss. The school School Business Manager holds a full copy of the act.

- Staff using electronic data relating to any student in the school should ensure that it is kept safe:
 - Where possible the computer that the data is held on should be protected by a password;
 - Backups of any data should be stored in a secure location;
 - Staff need to be aware that hard copies of data may contain sensitive information and should ensure that appropriate steps are taken.
- Staff are responsible for ensuring that there is no unauthorised access to electronic data when used off site. Precautions to guard against accidental loss should also be taken.
- Staff must avoid using electronic data relating to students on the Internet or when using E-mail services.

Staff must ensure that the appropriate form relating to off site data use (see example in handbook) has been filled in and passed to the School Business Manager.

Virus Protection

The ICT network has virus scanning installed; however, staff need to exercise due care and attention when using equipment outside of school and ensure that the appropriate virus scanning software is installed and kept up-to-date. Advice may be sought from the Network Manager or the Senior Leader responsible.

Health and Safety

All staff must be aware of health and safety issues associated with ICT.

ICT equipment should be located in an area that provides enough space to house the workstation, monitor, mouse and keyboard. There should be enough space for staff to rest their hands in front of the keyboard. When using a mouse staff should remember that intensive use could give rise to repetitive strain injuries. The key here is to exercise common sense with the positioning of the mouse, make sure it is easy to reach, support your forearm and make sure that you take a break during long periods of computer work.

Ensure that a suitable seat is chosen to alleviate issues relating to posture.

When siting ICT equipment make sure that there is sufficient lighting and that reflection and glare from windows/lighting is taken into consideration. The top of the monitor screen should be roughly at eye level, monitors should be able to be adjusted to suite the requirements of individual users. Staff should adjust contrast and brightness to meet their needs.

Staff should ensure that vents on ICT equipment are not obstructed.

If staff suspect a fault on ICT equipment, under no circumstances should they conduct anything other than a visual check. This should only occur if the appliance has been switched off and disconnected from the main supply. Staff should report any fault to the ICT support team using the ICT maintenance form provided or via email/telephone.

Any questions/concerns relating to ICT health and safety should be raised with the Health and Safety Officer or the School Business Manager.

Website

Staff need to ensure that only appropriate materials are published on the school website. Approval must be sought from the designated Senior Leader responsible prior to publication, who will then pass it to the school webmaster for publication.

Conformity to Legislation

All uses of ICT equipment/resources are subject to the relevant legislation. This includes the Data Protection, Computer Misuse and Designs, Copyright and Patents Acts. The School Business Manager holds copies of the Data Protection and Computer Misuse Acts, which staff can review at any time. Details of all legislation and online versions of each act are available via the Internet at www.legislation.hms.gov.uk.

Procurement of ICT Equipment

Purchases of new ICT equipment/resources must not be processed without consultation with the Network Manager. This is to ensure that where possible, the school operates on a common platform and that any ICT equipment is suitable.

Breach of Policy

All members of staff should be aware that a breach of any of the above by students or staff is serious and may lead to disciplinary action.

Monitoring, review and evaluation

The implementation of this policy is monitored by the Network Manager, the designated member of the SLT and the Headteacher. The policy will be reviewed every 2 years.