



# Hebburn Comprehensive School

## ICT Acceptable Use Policy

### 1. Overview

The purpose of this document is to ensure that all users of the school's computing facilities are aware of school policies relating to their use.

The document goes into some detail in the following three areas:

- Use of school hardware and software
- Use of the Internet and e-mail
- Misuse/disciplinary procedures

It is the responsibility of all users of the school computing facilities to be aware of and follow all school ICT policies and guidelines and to seek advice in case of doubt from ICT support staff or members of the SLT .

For the purpose of this overview, listed below are some key points:

- Only software properly purchased and/or approved by SLT/ICT Support may be used on the school's hardware. ICT Support will carry out installation of such software.
- Personal use of the Internet or e-mail should be restricted to times before 8:30am or after 3.00pm.
- Passwords protect the school's systems from access by unauthorised people. Therefore, staff must be careful to safeguard passwords at all times.
- 'All staff' e-mail messages should only be sent when the content is appropriate to all recipients and of relevance to many staff. In general e-mail messages should be sent only to particular individuals and groups.
- Where staff are working on documents that may need viewing by other colleagues, such documents should be stored on an appropriate Network directory rather than solely in the work area of the individual.
- Personal use of e-mail and the Internet between 8.30am and 3.00pm would constitute misconduct and could invoke the school's disciplinary procedures.
- The school reserves the right to carry out spot checks/monitoring of computer usage to include e-mail and internet history.

All staff will need to read through the document, sign the section at the end, and pass a copy onto SLT via John Attwood.

# Contents

	<b>Page</b>
<b>2. School Network, Hardware and Software</b>	<b>3</b>
2.1 Software	3
2.2 Data Security	3
2.3 Personal Data and the Data Protection Act	4
2.4 Freedom of Information Act	4
2.5 Virus Protection	4
2.6 Network Access	5
2.7 Further General Guidance	5
2.8 Laptops	5
<b>3 Electronic Mail</b>	<b>5</b>
3.1 Use and Responsibility	5
3.2 Content	5
3.3 Privacy	6
<b>4 Internet Usage</b>	<b>6</b>
<b>5 Private Use, Legislation and Disciplinary Procedures</b>	<b>7</b>
5.1 Private Use	7
5.2 Updates to this Policy	7
5.3 Disciplinary Action	
<b>Appendix 1:</b> Examples of behaviours which require the use of the school disciplinary policy	<b>8</b>
<b>Appendix 2:</b> Action to be taken in cases of suspected abuse of computers if gross misconduct is suspected	<b>9</b>
<b>Appendix 3:</b> Action to be taken in cases of suspected abuse of computers which does not constitute gross misconduct	<b>10</b>

## **2. The School Network, Hardware and Software**

Networked computers are a critical asset to the school and must be managed carefully to maintain security, data integrity and efficiency.

### **2.1 Software**

Only software properly purchased and/or approved by SLT/ICT Support may be used on the school's hardware. Non-standard or unauthorised software can cause problems with the stability of school's network and it is necessary to contact ICT Support who will carry out installation of such software, if it is deemed appropriate.

The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licences must always be adhered to. Do not ask ICT support or other members of staff to copy software or music that is copyrighted or un-licensed.

Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above are encouraged to contact ICT Support who will be happy to assist in resolving any issues.

### **2.2 Data Security**

Under no circumstances should you disclose personal or other confidential information held on a computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

It is school policy to store data on a network drive where it is regularly backed up. You must ensure that data that is not stored on the network server is regularly backed up.

Where staff are working on documents that may need viewing by other colleagues, such documents should be stored on an appropriate Network directory rather than solely in the work area of the individual.

### **2.3 Personal Data and the Data Protection Act**

The school maintains a notification to the Data Protection Commission in compliance with the Data Protection Act 1998. This notification is held on a public register and contains details of the organisations holding and processing of personal data.

The Data Protection Compliance officer must be informed of all collections of personal data through the annual audit. It is the responsibility of all school staff to ensure that personal data is held and processed within the terms of the school notification and in compliance with the data protection principles.

Personal data shall be:

- Obtained and processed fairly and lawfully
- Held for specified lawful purpose(s)
- Not used or disclosed in a way incompatible with the purpose(s)
- Adequate, relevant and not excessive for the purpose(s)
- Accurate and up to date
- Not kept longer than necessary
- Available to the data subject
- Kept secure.

Staff should note that all data and correspondence, including e-mail messages, held by the school may be provided to a data subject, internal or external, in the event of a subject access request.

### **2.4 Freedom of Information Act**

The school is subject to the provisions of the Freedom of Information Act (2000) which provides for the general right of access to information held by public authorities. While the school is in the process of meeting the requirements of the Act, employees should be aware that the Act effectively extends rights available under the Data Protection Act to include all types of information held, whether personal or non-personal. Therefore, such data or correspondence may be provided to an applicant in the event of an access request. Further information about this Act may be obtained from SLT .

### **2.5 Virus Protection**

Anti-virus software is loaded on all computers as standard and is updated regularly via the network. Anti-virus software must not be de-installed or deactivated. Files received by or sent by e-mail are checked for viruses automatically.

Users must not intentionally access or transmit computer viruses or similar software.

If you suspect that a virus has infected a computer then stop using the computer and contact ICT Support immediately.

## **2.6 Network Access**

Passwords protect the school's systems from access by unauthorised people: they protect the work of staff and pupils as well as school information, some of which may be sensitive and confidential. Therefore, be careful to safeguard this password at all times.

The school does not allow the connection of external computer equipment to the network without prior consultation from ICT Support.

## **2.7 Further General Guidance**

School hardware must not at any time be used for external business interests or personal gain.

## **2.8 Laptops**

Laptops are provided for school business. The private use of laptops outside of school hours is permissible, but with a view to the content of Appendix 1. Staff need to be aware that they are responsible for any files downloaded on to their laptop even if that may be done by another family member.

# **3. Electronic Mail**

## **3.1 Use and Responsibility**

The school's electronic mail (e-mail) system is provided for the School's business purposes. E-mail is now a critical tool but inappropriate use can expose the school and the user to significant liability. Liability can arise in a number of ways including, among others, copyright or trademark infringement, misuse of confidential information, defamation and liability for inaccurate statements.

All staff e-mail messages should only be sent when the content is appropriate to all recipients and of relevance to many staff. In general e-mail messages, should be sent only to particular individuals and groups.

### **3.2 Content**

E-mail messages must be treated like any other formal written communication.

E-mail messages cannot be considered to be private, secure or temporary. E-mail can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

Improper statements in e-mail can give rise to personal liability and liability for the school and can constitute a serious disciplinary matter.

Do not create or send e-mail messages that are defamatory. Defamatory e-mails whether internal or external can constitute a published libel and are actionable.

Do not create or send e-mail messages that may be intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability.

It is never permissible to subject another employee to public humiliation or ridicule; this is equally true via e-mail.

Copyright law applies to e-mail. Do not use e-mail to transmit or circulate copyrighted materials.

### **3.3 Privacy**

E-mail messages to or from you cannot be considered to be private or confidential. Although it is not policy to routinely examine the content of individuals e-mail, the school reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or some legal obligation to do so. Good cause shall include the need to fulfil School obligations, detect employee wrong doing, protect the rights or property of the School, protect ICT system security or to comply with legal process.

Messages sent or received may be copied and disclosed by the School for lawful purposes without prior notice.

It is not permissible to access or to send e-mail from another employee's personal account either directly or indirectly, unless you obtain that person's prior written approval.

## **4. Internet Usage**

The overriding principle guiding the use of the internet is that it must not breach professional standards that are clearly essential and expected in a school responsible for the education, well-being and safeguarding of young children.

All internet usage from the school network is monitored and logged. Material regarded as offensive under English law must not be accessed or published on the internet. Such material would include content concerning sex, race, colour, religion, etc. Deliberate access or publishing of offensive material would constitute misconduct and would invoke the school's disciplinary procedures and possible criminal investigation. Copyright and licensing conditions must be observed when downloading software or other material from the internet.

## **5. Private use, legislation and disciplinary procedures**

### **5.1 Private Use**

Computing facilities are provided for the school business purposes and responsible personal use is allowed provided there is no conflict with the interests or requirements of the school.

Personal use of the Internet or e-mail should be restricted to times before 8:30am or after 3:00pm. on school networked computers.

### **5.2 Updates to this Policy**

In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available.

### **5.3 Disciplinary Action**

The school wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently it expects and supports the integrity of its staff.

In exceptional circumstances, where there are reasonable grounds to suspect that a member of staff has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

**Appendix 1** gives detailed examples of behaviours which are unacceptable within the school and provides examples of behaviour deemed as Gross Misconduct and Misconduct.

**Appendix 2** provides a Flowchart of action to be taken in cases of suspected abuse of computers that constitute Gross Misconduct.

**Appendix 3** provides a Flowchart of action to be taken in cases of suspected abuse of computers that constitute Misconduct.

**Appendix 1:**  
**Examples of behaviours which require the**  
**use of the school disciplinary policy**

**GROSS MISCONDUCT** Examples:

- 1 Acts – for example in relation to child pornography.
- 2 Visiting pornographic sites except where this forms an authorised part of the employees job.
- 3 Viewing sexually explicit materials, except where this forms an authorised part of the employees job.
- 4 Harassment – inappropriate e-mails or printed e-mails sent to a colleague, even if sent as a joke. Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace.
- 5 Obscene racist jokes or remarks which have been shared internally and externally – reflects on the image of employer and brings the organisation into disrepute.
- 6 Using Chat Rooms – sexual discourse, arrangements for sexual activity.

**MISCONDUCT** Examples:

- 1 Personal use of e-mail and the Internet between 8.30am and 3.00pm.
- 2 Frivolous use of School computing facilities that risk bringing the school into disrepute. The distribution of ‘chain e-mails’ beyond the internal e-mail system would represent examples of such misconduct.
- 3 Entering into contracts via the Internet that misrepresent the school. Contracts are legally binding agreements and members of staff must not enter into any agreements via the Internet to procure goods or services where the school is liable for this contract, without first consulting the School Business Manager.
- 4 Deliberate introduction of viruses to systems.
- 5 Downloading and installation of unlicensed products.
- 6 Violation of the schools registration with the Federation Against Software Theft – such as software media counterfeiting or illegitimate distribution of copied software.

This list is not exhaustive, but sets the framework of the school’s approach to misuse of computing systems. The school has the right to monitor staff use of computer equipment where there is evidence to suggest misuse. (Regulation of Investigatory Powers Act 2000).

## **Appendix 2: Action to be taken in cases of suspected abuse of computers if gross misconduct is suspected**

Where a manager suspects misuse or where a member of staff has concerns about a colleague:

- Discuss with appropriate line manager
- Refer to SLT for information

Following discussion, and if considered appropriate, SLT to contact the Network Manager to provide data on the individual's use of the computer network.

SLT will make a judgement based on information available as to whether investigation is necessary and will discuss evidence with the line manager.

If so, the Head Teacher will:

- Discreetly stop the employee from further use of the network.
- Ask the member of staff to attend an interview with a colleague in attendance.

### **Suspension Interview**

The Head Teacher supported by SLT will give brief details of what is suspected and suspend the employee from work to allow further investigation. Suspension will be on full pay.

The employee will be escorted from the premises and told to refrain from work until further notice. They will not be allowed to attend the premises until asked to do so by the Head Teacher and will be excluded from using any equipment or property of the school.

### **Decision to advise the Police for Criminal Investigation**

On the facts that are immediately available, a decision will be taken whether to refer the matter to the Police for criminal investigation. This does not preclude the matter being referred to the Police at any later stage when a formal investigation has been undertaken within the disciplinary procedure.

### **The School Disciplinary Procedure**

SLT will then continue a formal investigation and the school disciplinary policy will be adhered to where required.

**Appendix 3:**  
**Action to be taken in cases of suspected abuse of computers  
which does not constitute gross misconduct**

Where a manager suspects misuse or where a member of staff has concerns about a colleague:

- Discuss with appropriate line manager
- Refer to SLT for information

Carry out preliminary investigation by asking the employee for an explanation and make other enquiries and investigate as required. At the conclusion of the investigation:

- enter the Gross Misconduct Investigation Procedure described in Appendix 2, or
- make a judgement that a verbal warning is needed, or
- enter the Disciplinary Process and convene a Disciplinary Hearing, or
- decide there is no case to answer and the matter concludes.