



ICT Usage Policy

ICT Usage Policy
Ratification Date: December 2015
Reviewed: As required
Next Ratification: December 2018
Governor/Director Owner: Chair of Operations Committee
Lead Staff Member Owner: Operations Director

Contents

Section	Page
1. Scope	3
2. Purpose	3
3. Policy	3
4. Access	3
5. Monitoring	3
6. Personal Use	4
7. Inappropriate Use	4
8. Authority to Express Views	4
9. Confidentiality and Security of Data	4
10. Copyright, Legal and Contractual Issues	5
11. Network Efficiency	5
12. Software	5
Appendix 1 – Statement of Acceptance of the Terms and Conditions of ICT Usage Policy	6

1. Scope

This policy applies to school based employees who are directly employed by the school. It applies to all users of the school's network, and the use of the school's facilities, (including telephones, hardware, software, e-mail, internet, mobile devices and WIFI, etc.) used anywhere, for professional or personal purposes, whether in working time or in the employee's own time.

2. Purpose

The purpose of this policy is to:

- Protect employees by making clear what is acceptable use of the Trust's computer facilities
- Protect the security and integrity of the school and its computer facilities

3. Policy

High standards of conduct and probity are as relevant to the use of the school computer facilities as they are to all other aspects of work and employees must conduct themselves in line with the school's code of conduct and disciplinary code.

Employees who are in any doubt about what is, or is not, acceptable use of the school's computer facilities must seek advice from their line manager.

Breach of this policy may lead to disciplinary action and result in withdrawal of access to some or all computer facilities. Serious breaches may be regarded as gross misconduct and may lead to dismissal. Employees are required to sign a statement agreeing to the terms and conditions of this policy (Appendix 1).

The school will co-operate with any law enforcement activity.

Managers must ensure that employees have the skills to use the school's computer facilities.

4. Access

The school provides access to ICT to enable employees to undertake their duties.

The Executive Headteacher and relevant Heads of School have authority to obtain access to any employee's data and documents.

5. Monitoring

Each employee will be required to sign the Statement of Acceptance of the Terms and Conditions of the ICT Usage Policy.

The school's computer facilities will be monitored to ensure this policy is adhered to and that these facilities are used properly.

Any information (including personal emails, document, etc.) within the school's network or equipment can be inspected at any time without notice.

6. Personal Use

Employees can use the school's computer facilities for reasonable personal use provided it:

- Does not interfere with the performance of their duties
- Is appropriate
- Is on an occasional, rather than a regular or substantial basis
- Does not compromise the security of the school's system or reputation

7. Inappropriate Use

Employees must not use the school's computer facilities to:

- Send or access messages that are, or perceived to be, libellous, harassing or defamatory, or cause offence to the dignity of an individual or group.
- Access inappropriate internal sites or material. These may include pornographic, racist or any other sites not appropriate for a school. In the case of accidental access, the employee must immediately disconnect and inform their line manager.
- Store, view, print or redistribute any inappropriate material.
- Access chat rooms, social networking sites or newsgroups for personal use.
- Advertise or send personal messages to large groups internally or externally unless through a specified facility or with the permission of the Headteacher.
- Spread harmful programmes that may damage the school's computer facilities.
- Download, use or distribute software including entertainment software or games.
- Download video and audio streaming for personal purposes.
- Use their school email address for the purchase of personal goods or financial transactions.

8. Authority to Express Views

Employees using school computer facilities must communicate the school's, and not their personal, views.

Employees must not participate in newsgroups/chat rooms/social networking sites, unless in a professional capacity relevant to their duties and with prior agreement from the Headteacher.

Employees must not use the school or its name to endorse any non-school commercial product or service.

9. Confidentiality and Security of Data

The Trust is legally responsible for all information stored or transmitted by its computer systems and for any improper disclosure. Disclosure of data, even unintentionally, can breach the Data Protection Act. Security measures are in place to ensure the confidentiality of data held by the school and employees are accountable for breaches of security or confidentiality.

- Employees must not attempt to disable or evade any security facility.

- User IDs and passwords must be kept secure and confidential and passwords changed if an unauthorised person may be aware of them.
- Employees must carefully address emails to avoid sending sensitive information to the wrong recipient.
- Employees must ensure that data they are storing, updating or transmitting is accurate, and must not amend or alter emails they receive.
- Employees must use the appropriate system/method e.g. password-protect screen saver, if leaving their computer for short periods and switch computers off at the end of the working day.

10. Copyright, Legal and Contractual Issues

Downloading and copying data and software or sending the work of others to third parties without permission can infringe copyright. The school retains the copyright to any original ICT based material produced by an employee in the course of their duties.

- Copyright should be checked and appropriate permissions sought. In the case of subscription services the appropriate licenses must be obtained.
- Software can only be downloaded with permission from the Headteacher or the designated authorised ICT person. Downloaded software becomes the school's property and must be used only under the terms of its license. Employees must arrange to license and register such software, where required. Software downloaded without permission must be deleted.
- Employees must not transfer any software licensed to the school or data owned or licensed by the school without authorisation from the Headteacher or the designated ICT person.
- The use of computer facilities can lead to contractual obligations in the same way as verbal or written transactions. Employees must not exceed their delegated authority to enter into contracts or authorise expenditure.

11. Network Efficiency

Employees must regularly delete or archive files no longer required or needed for immediate access.

The school's ICT unit will scan all files for viruses.

Where possible intensive operations such as large file transfers, video downloads, mass emailing should be scheduled during off-peak hours.

Video and audio streaming and downloading must be for work purposes only.

12. Software

The school must ensure all software is legally licensed and is responsible for managing and maintaining the register of software and for holding licenses and the original media.

- No software can be loaded onto or used on any computer owned or leased unless approved by and licensed to the school.
- All software must be procured by the school and installed by the designated authorised ICT person.
- Software must not be copied or distributed by any means without prior approval from the Headteacher or the designated authorised ICT person.

Statement of Acceptance of the Terms and Conditions of the ICT Usage Policy

I agree to follow the rules set out in the ICT Usage Policy. I will use the network in a responsible way and observe all the restrictions explained in the Policy. If I am in any doubt I will consult the Headteacher.

I agree to report any misuse of the school's ICT network to the Headteacher.

I also agree to report any websites that are available on the school internet that contain inappropriate material to the Headteacher.

I understand that any breaches of the Policy may result in loss of access to the ICT resources and can be subject to disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Name of Employee:

Signature of Employee:

Date: