

ICT Usage Policy

Category:	Trust-wide Policy
Authorised By:	Board of Trustees
Author:	Sumit Parmar, <i>ICT Manager</i>
Owner:	Sudhi Pathak, COO
Version:	8
Status:	Ratified
Issue Date:	March 2026
Next Review Date:	March 2027

Version Control

<u>Ver.</u>	<u>Date</u>	<u>Comment</u>
2	May 2019	
3	March 2021	Academised version of Schools' HR model
4	April 2022	Cyclical review. Updates working from home and download of data to home devices to reflect the use of Cloud services
5	March 2023	Cyclical review.
6	March 2024	Cyclical review. No changes.
7	March 2025	Cyclical review.
8	March 2026	Cyclical review. No substantive changes

This policy will be subject to ongoing review and may be amended prior to the scheduled date of the next review in order to reflect changes in legislation, statutory guidance, or best practice (where appropriate).

Contents

1. Scope.....	4
2. Purpose.....	4
3. Policy	4
4. Access	5
5. Monitoring	5
6. Inappropriate use	5
7. Personal use of trust equipment.....	6
8. Use of Personal devices to access Trust's Office 365 system and emails	6
9. Authority to express views.....	6
10. Confidentiality and security of data	7
11. Copyright, legal, and contractual issues.....	7
12. Network efficiency.....	8
13. Software	8
Appendix: Statement of acceptance of the terms and conditions of the ICT Usage Policy and Social Media Policy	9

1. Scope

The procedure applies to all staff directly employed by the Trust. It also applies to all Members, Trustees and LAB/Committee members across the Trust.

It applies to all users of the Trust's¹ network and the use of the Trust's ICT facilities, (including telephones, hardware, software, e-mail, internet etc) used anywhere, for professional or personal purposes whether in working time or in the employee's own time.

Please refer to the Social Media section of the IT & Online Safety Policy for further guidance on the use of social networking sites and other technology.

2. Purpose

The purpose of this policy is to:

- Protect employees by making clear what is acceptable use of the school's ICT facilities.
- Protect the security and integrity of the school and its ICT facilities and all personal data.

3. Policy

High standards of conduct and probity are as relevant to the use of the Trust's ICT 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 Trust's ICT facilities must seek advice from their Head², line manager or the ICT manager in advance of the use.

Employees must conduct themselves honestly, appropriately and in accordance with the law and this policy when using the Trust's ICT facilities.

Breach of this policy may lead to disciplinary action and result in withdrawal of access to some or all ICT 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).

Managers must ensure that employees have the relevant skills to use the Trust's ICT facilities.

The Trust will purchase all hardware and software through approved suppliers.
The Trust will co-operate with any law enforcement activity.

¹ For the purposes of this Policy, all references to the Trust's equipment, infrastructure, systems etc. refers also to the same at any of the Trust's schools

² For the purposes of this policy, Head refers to Executive Head, Headteacher or Head of School/Setting/Satellite as appropriate

4. Access

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

The CEO, Deputy CEO, COO or Head or another designated senior person has authority to obtain access to an 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 Trust's ICT facilities will be monitored to ensure this policy is adhered to and that these facilities are used properly.

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

6. Inappropriate use

Employees must not use the Trust's ICT 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 internet 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 Head or 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 an authorised person.
- 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. In addition:
- Staff must not use their school e-mail address for the purchase of personal goods or financial transactions.
- The use of portable removable devices including memory sticks is prohibited on the school network, unless approved first by the Head or ICT Manager. Any removable devices must be fully encrypted.
- Staff must not to share passwords or allow anyone else access to their network account and must not give their family members access to Trust's ICT facilities (devices, systems or accounts, including school laptops)

- When staff access the Trust's IT network from home, they must ensure family members are unable to see any documents that belong to the Trust.
- Any device being used must be locked when staff are not using that device.
- Any documents that have been downloaded via the Trust's IT network and being used on a home device, must be deleted from the device once the staff member has finished working on it.

7. Personal use of trust equipment

Employees can use the school's ICT facilities for occasional 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 Trust's systems or reputation.

8. Use of Personal devices to access Trust's Office 365 system and emails

Use of personal devices to access the Trust's documents via office 365 should be avoided where possible

If a personal device is used to access the Trust's documents then the personal device should be password protected and have anti-virus installed.

The user should log out from the Trust's office 365 system after using their personal device

Trust Emails are permitted to be used on personal mobile devices as long as the device has an appropriate security lock in the form of bio metric, pin code or an alphanumeric code.

Access to emails can be via an appropriate app on the mobile device or the browser.

Emails should not be accessed on shared mobile devices, in those instances where this is unavoidable, you need to log out of your email account in each occasion.

Trust GDPR policies also apply to personal devices and emails.

9. Authority to express views

Employees using the Trust's ICT 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 their manager or the designated authorised person.

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

10. 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 General Data Protection Regulations 2018 and Data Protection Act 2018.

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 e-mails 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 e-mails they receive.

To ensure security, it may be necessary to prevent equipment with sensitive data from connecting to the internet or restrict usage of file transfers.

Employees must use the appropriate system/method e.g., password-protected screen saver, if leaving their computer for short periods and switch computers off at the end of the working day.

Trustees, Members, independent committee members and Local Advisory Board members should use their designated Trust email account for all matters concerning Trust/school business.

Equipment and devices provided by the Trust for work purposes should only be used by the employee who has been assigned the equipment. The employee must at all time use all reasonable efforts to keep the equipment secure off site.

11. 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 Trust 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 CEO, Deputy CEO, COO, Head or the ICT Manager.

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 Trust or data owned or licensed by the Trust without authorisation from the CEO, Deputy CEO, COO, Head or the ICT Manager.

The use of ICT 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.

Records of computer transactions must take place through archiving or backup. Where appropriate, confirmation of receipt of important e-mails must be gained which may be disclosed in litigation.

Transactions through any ICT facility must be treated in the same way as transactions on the school's headed paper.

12. Network efficiency

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

The Trust's ICT Manager will arrange for scans of all files for viruses.

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

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

13. Software

The Trust 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 Trust.

All software must be procured by the Trust and installed by the ICT Manager.

Software must not be copied or distributed by any means without prior approval from the Head or the ICT Manager.

Appendix: Statement of acceptance of the terms and conditions of the ICT Usage Policy and Social Media Policy

I agree to follow the rules set out in the ICT Usage Policy.

I will use the school's ICT network in a responsible way and observe all the restrictions explained in the Policy. If I am in any doubt, I will consult the Head (for schools) or Chief Operating Officer (for central staff).

I agree to report any misuse of the school's ICT network to the Head (for schools) or Chief Operating Officer (for central staff).

I also agree to report any websites that are available on the school Internet that contain inappropriate material to the Head (for schools) or Director of Finance & Operations (for central staff).

I understand that any breaches of the policy may result in loss of access to the ICT facilities and will 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.

I have also read and agree to the Trust's IT and Online Safety Policy (incorporating the Social Media Policy) and agree with the terms and conditions outlined in that, namely:

- I agree to follow the rules set out in the Social Media Policy.
- I will use all relevant social media and the Trust's network and ICT facilities in a responsible way so as to preserve and protect the interest of the school at all times and will observe all the restrictions explained in the Policy. If I am in any doubt, I will consult the Head or the Trust's ICT Manager.
- I agree to report any misuse or a breach of this policy to the Head or the Trust's ICT Manager.
- I understand that any breaches of the Policy may result in disciplinary action being taken against me.

Name of employee

Signature of employee

Date