



ICT Responsible Use Policy

Version	1.2
Approving Body	Trust Board
Date ratified	13 July 2026
Date issued	1st September 2026
Review date	30th September 2029
Owner	Director of People & Culture
Applies to	All Trust Schools, all Trust staff

Version	Date	Reason
1.0	October 2020	To establish a Trust wide policy
1.1	October 2023	Periodic review. Removal of appendix 1
1.2	September 2026	Periodic review, appendix added.

Contents

- 1. Introduction 2
- 2. Scope and purpose 3
- 3. Monitoring 3
- 4. Policy rules 4
- 5. Review of policy 9
- Appendix - Equality Impact Assessment

1. Introduction

1.1 ICT is provided to support and improve the teaching and learning in our Trust as well as ensuring the smooth operation of our administrative and financial systems.

1.2 This policy sets out our expectations in relation to the use of any computer or other electronic device on our network, including how ICT should be used and accessed within the Trust.

1.3 The policy also provides advice and guidance to our employees on the safe and acceptable use of social media. The acceptable use of ICT will be covered during induction and ongoing training will be provided, as appropriate.

1.4 This policy does not form part of any employee's contract of employment and may be amended at any time, however a breach of this policy is likely to result in disciplinary action.

2. Scope and purpose

2.1 This policy applies to all employees, Trustees, Local School Committee members, volunteers, visitors and any contractors using our ICT facilities. Ensuring ICT is used correctly and properly and that inappropriate use is avoided is the responsibility of every employee. If you are unsure about any matter or issue relating to this policy you should speak to your line manager, or a senior member of staff.

2.2 The purpose of this policy is to ensure that all employees are clear on the rules and their obligations when using ICT to protect the Trust and its employees from risk.

2.3 Employees may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

2.4 Any failure to comply with this policy may be managed through the disciplinary procedure. A serious breach of this policy may be considered as gross misconduct which could lead to dismissal. If we are required to investigate a breach of this policy you will be required to share relevant password and login details.

2.5 If you reasonably believe that a colleague has breached this policy you should report it without delay to your line manager or a senior member of staff.

3. Monitoring

3.1 The contents of our ICT resources and communications systems held in whatever media, including information and data held on computer systems, hand-held devices, tablets or other portable or electronic devices and telephones, relating both to the Employer's own educational provision or any pupils, clients, suppliers and other third parties with whom the Employer engages or provides educational provision for, remains our property. Therefore, employees should have no expectation of privacy in any message, files, data, document, facsimile, social media post, blog, conversation or message, or any other kind of information or communication transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems. Do not use our ICT resources and communications systems for any matter that you wish to be kept private or confidential.

3.2 We may monitor, intercept and review, without notice, employee activities using our ICT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and are for legitimate business purposes. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

3.3 We will comply with the requirements of **Data Protection Legislation** (being (i) unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 2018) in the monitoring of our IT resources and communication systems and monitoring undertaken is in line with our Workforce Privacy Notice which sets out how we will gather, process and hold personal data of individuals during their employment. Our Data Protection Policy sets out how we will comply with Data Protection Legislation.

3.4 In line with the requirements of Data Protection Legislation, we may store copies of data or communications accessed as part of monitoring for a period of time after they are created, and may delete such copies from time to time without notice. Records will be kept in accordance with our Data Protection Policy.

4. Policy rules

4.1 In using the Trust's ICT resources, the following rules should be adhered to.

4.2 The network and appropriate use of equipment

(a) You are permitted to adjust computer settings for comfort and ease of use.

(b) Computer hardware has been provided for use by employees and pupils and is positioned in specific areas. If there is a problem with any equipment or you feel it would be better sited in another position to suit your needs, please contact your school's ICT lead. Only the school's ICT lead should move or adjust network equipment.

(c) Do not disclose your login username and password to anyone (unless directed to do so by a senior manager for monitoring purposes or as stated in clause 2.4).

(d) You are required to change your password in accordance with the login prompts. Ensure that you create appropriate passwords as directed.

(e) Do not allow pupils to access or use your personal logon rights to any school system.

(f) Before leaving a computer, you must log off the network or lock the computer, checking that the logging off procedure is complete before you leave.

(g) Ensure projectors linked to the network are switched off when not in use.

(h) Only software provided by the network may be run on the computers. You should liaise with your school's ICT lead before importing or download applications or games.

(i) You must not use any removable storage devices (RSDs), such as USB pens where you are unsure of the content or origin.

(j) Pupil or staff data, or any other confidential information should not be stored on a RSD.

(k) RSDs should only be used for Trust purposes, outside of our premises where they are encrypted.

4.3 Mobile devices and laptop use

1. The following rules are for use of any laptop, electronic tablets, mobile phone or other mobile device used for Trust or school activity, including those provided by the Trust. Referred to as mobile device(s):

(a) Access to our wireless network must be approved by the Trust ICT Team.

(b) You must ensure that your mobile device is password/PIN or biometrically protected.

(c) You must not leave your mobile device in an unsafe place, for example in your car.

(d) You must have appropriate security in place and it must be updated regularly. For instance you should ensure that your device has adequate virus protection.

4.4 Internet safety

(a) Never give out personal information such as your address, telephone number or mobile number over the internet without being sure that the receiver is from a reputable source.

(b) Never give out personal information about a pupil or another employee over the internet without being sure that the request is valid and you have the permission to do so.

(c) Always alert the Trust ICT Team if you view content that makes you feel uncomfortable or you think is unsuitable. Remember that any personal accounts accessed on our network will be subject to monitoring.

(d) Always alert the Trust ICT Team if you receive any messages that make you feel uncomfortable or you think are unsuitable.

4.5 Internet and email

(a) The internet and email facilities are provided to support the aims and objectives of the Trust. Both should be used with care and responsibility.

(b) Use of the internet at work must not interfere with the efficient running of the Trust. We reserve the right to remove internet access to any employee at work.

(c) You must only access those services you have been given permission to use.

(d) Before sending an email, you should check it carefully and consider whether the content is appropriate. You should treat emails like you would any other form of formal written communication.

(e) Although the email system is provided for business purposes we understand that employees may on occasion need to send or receive personal emails using their work email address. This should be kept to a minimum and should not affect, or be to the detriment of, you carrying out your role effectively. When sending personal emails from your work email

account you should show the same care in terms of content as when sending work-related emails.

(f) The use of email to send or forward messages which are defamatory, obscene or otherwise inappropriate may be dealt with under the disciplinary procedure.

(g) You should not send electronic messages which are impolite, use obscene language, are indecent, abusive, discriminating, racist, homophobic or in any way intended to make the recipient feel uncomfortable. This will be considered under the disciplinary procedure.

(h) If you receive an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, you should not forward it to any other address but you should alert the Trust ICT Team.

(i) Do not access any sites which may contain inappropriate material or facilities, such as:

- (i) Unauthorised proxy/VPN
- (ii) Dating
- (iii) Hacking software
- (iv) Pornographic content
- (v) Malicious content
- (vi) Music downloads
- (vii) Non-educational games
- (viii) Gambling

(j) Do not send malicious or inappropriate pictures of children or young people including pupils, or any pornographic images through any email facility. If you are involved in these activities the matter may be referred to the police.

(k) Under no circumstances, should you view, download, store, distribute or upload any material that is likely to be unsuitable for children or young people. This material includes, but is not limited to pornography, unethical or illegal requests, racism, sexism, homophobia, inappropriate language, or any use which may be likely to cause offence. If you are not sure about this, or come across any such materials you must inform the Trust ICT Team.

(l) Do not upload or download unauthorised software and attempt to run on a networked computer; in particular hacking software, encryption and virus software.

(m) Do not use the computer network to gain unauthorised access to any other computer network.

(n) Do not attempt to spread viruses.

(o) Do not transmit material subject to copyright or which is protected by trade secret which is forbidden by law.

(p) Never open attachments of files if you are unsure of their origin; delete these files or report to the Trust ICT Team.

(q) If you are unsure about whether you have the owner's permission do not download or use any material from the internet.

4.6 Social networking and use of the chatrooms, community forums and messaging using

any device

The internet provides unique opportunities to participate in interactive discussions and share information using a wide variety of social media. Employees' use of social media can pose risks to our ability to safeguard children and young people, protect our confidential information and reputation, and can jeopardise our compliance with our legal obligations. This could also be the case during off duty time.

- (a) You should exercise caution when using social networks. You should not communicate with pupils over social network sites. You must block unwanted communications from pupils. You are personally responsible for what you communicate on social media.
- (b) You should never knowingly communicate with pupils in these forums or via personal email account or personal mobile phones.
- (c) You should not interact with any ex-pupil of the Trust who is under 18 on such sites.
- (d) Communication with pupils should only be conducted through our usual channels. This communication should only ever be related to our business.
- (e) You must not post disparaging or defamatory statements about:
 - (i) our Schools and Trust;
 - (ii) our pupils, parents or carers;
 - (iii) our Trustees, Local School Committee members or employees;
 - (iv) other affiliates and stakeholders.
- (f) You should avoid communications that might be misconstrued in a way that could damage our reputation, even indirectly.
- (g) You should make it clear in social media postings that you are speaking on your own behalf. Write in the first person and use a personal email address when communicating via social media.
- (h) If you disclose that you are an employee of our Trust, you must also state that your views do not represent those of your employer. You should also ensure that your profile and any content you post are consistent with the professional image you present to pupils and colleagues.
- (i) You must not access social networking sites for personal use via our information systems whilst at work.
- (j) Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to our Trust are also prohibited.
- (k) Remember that what you publish might be available to be read widely by others (including us, future employers and acquaintances) for a long time. Keep this in mind before you post content.

4.7 The following acts are prohibited in relation to the use of the ICT systems and will not be tolerated:

- (a) Violating copyright laws

- (b) Attempting to harm minors in any way
- (c) Impersonation of any person or entity, or to falsely state or otherwise misrepresent an affiliation with a person or entity
- (d) Forging headers or otherwise manipulating identifiers in order to disguise the origin of any content transmitted through any internet service
- (e) Uploading, posting, messaging or otherwise transmitting any content without the right to transmit under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements)
- (f) Uploading, posting, messaging or otherwise transmitting any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party
- (g) Uploading, posting, messaging or otherwise transmitting any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes", or any other form of solicitation.
- (h) "Stalking" or otherwise harassing any user or employee
- (i) Collection or storage of personal data about other users

5. Review of policy

5.1 This policy is reviewed every three years by the Trust unless technological changes warrant a review. We will monitor the application and outcomes of this policy to ensure it is working effectively.

Equality Impact Assessment/ Analysis (EIA)

Step 1: Scoping and Identifying the Aims

School/Service	People Department
Title of Change:	ICT responsible use Policy
What are you completing this EIA for?	Policy
Is this a new or existing activity or change?	Existing
What are the main aims / objectives of the changes?	Ensure policy is still relevant and the most current legislation is being adhered to.
What is the context for this EIA? e.g., policy, practice, service, curriculum proposal or project?	
Why is the activity/change needed? E.g., The policy or practice affect different "protected groups" differently?, enhancing of services, education	
Name/s of people and Date undertaking analysis:	Shani Davies, Director People & Culture
Who will be affected by this activity/change? eg pupils/students, service users, employees, wider community	All Staff in scope of this policy
Does it relate to an area with known inequalities? E.g., access to service for disabled people, pupils/students, vulnerable pupils/students, SEND, racist bullying etc.	
EIA Schedule When will the EIA be reviewed?	

Step 2: Assessing the Impact

Detail any positive or negative impacts of this document /policy on pupils/students and staff in the box below. If there is no impact, please select "not applicable"

Protected Characteristic	Positive Impact(s)	Negative Impact(s)	NA	Action to address negative impact: (e.g. adjustment to the policy)
Sex consider issues for: men and women, non-binary.	Y			
Gender reassignment E.g. privacy of data and harassment	Y			
Disability e.g., attitudes, physical, social barriers, visible and non-immediately visible disabilities, neurodivergence, learning disability	Y			
Age e.g., consider all ages but there may be some issues that relate for example to older people/younger people	Y			
Sexual Orientation consider heterosexual as well as lesbian, gay and bisexual (and other sexual orientations)	Y			
Pregnancy and maternity e.g., childcare, working arrangements, part time working	Y			

Marriage and civil partnership	Y			
Religion or belief consider religions, beliefs, or no belief	Y			
Ethnicity / Race e.g., language barriers, different ethnic groups/nationalities	Y			
Socio-economic factors e.g., resident status – socio economic/low-income groups, migrants, carers, impacts on children and families (please state)	Y			
Mental health e.g. short term, long term, acute, fluctuating mental health conditions, impacts	Y			

If you answer yes to any of the following, you MUST complete the evidence column explaining what information you have considered which has led you to reach this decision.

Assessment Questions	Yes / No	Please document evidence / any mitigations
In consideration of your document development, did you consult with others, for example, external organisations, employees, pupils/students, carers or community groups?	Yes	Staff and Trade Unions
Have you taken into consideration any regulations, professional standards?	Yes	Equality Act 2010, UK GDPR, Data Protection Act 2018, WCAG 2.2, DfE Digital Standards 24-26, ICO, public sector bodies accessibility regulations 2018, KCSIE 25'

Step 3: Review, Risk and Action Plans

Low – No major change	Medium - Adjust the policy	High – Stop and remove
The activity is robust and there is no potential for discrimination, and you have taken all appropriate opportunities to advance and foster relations between groups.	This involves taking steps to remove barriers or to better advance equality. It can mean introducing measures to mitigate the potential effect.	If there are adverse effects that are not justified and cannot be mitigated, you will want to consider stopping the policy/project altogether. If the activity shows unlawful discrimination, it must be removed or changed.

How would you rate the overall level of impact / risk to the school / service / Trust if no action was taken?	Low x ☐	Medium ☐	High ☐
What action needs to be taken to reduce or eliminate the negative impact?	N/A		
Who will be responsible for monitoring and regular review of the document / policy / change?	Director People & Culture		

Step 4: Authorisation and sign off

I am satisfied that all available evidence has been accurately assessed for any potential impact on pupils/students and employees with protected characteristics in the scope of this project / change / policy / procedure / practice / activity. Mitigation, where appropriate has been identified and dealt with accordingly.

Equality Assessor:	Shani Davies	Date:	22/4/26
---------------------------	---------------------	--------------	---------

