David Ross Education Trust

Broadening Horizons

Acceptable Use Policy – Staff

Document Management Information

Applicable to:	All staff in all Academies and Central Support Services including individuals employed by the Trust, contractors and agency staff. All Members and Trustees.
Dissemination:	The policy will be available to staff via the Trust's Policy Centre
Implementation:	Applicable to all DRET academies
Training:	Mandatory induction and periodic refresher training, with additional role-specific training where required.
Review Frequency:	The policy will be reviewed every three years. The policy will also be reviewed earlier if needed in the light of new evidence/legislation/guidance
Policy Author:	George Selby, Head of Data Protection and Compliance
Executive Policy Owner:	Maria Maltby, Director of Governance
Approval by:	Level 3 (Executive)
Approval Date:	19 October 2026
Next Review Due:	October 2029

Revision History

Document version	Description of Revision	Date Approved
V0.1	Draft for Executive review	May 2020
V1.0	Approved version	22 June 2020
V1.1	Amended to reflect Brexit and change from GDPR to UKGDPR	21 Jan 2021
V1.2	Executive review	25 April 2023
V1.3	Amended to reflect changes to streaming accounts	2 December 2025
V1.4	Inclusion of AI provisions and strengthening of safeguarding	19 October 2026

Contents

Contents 3
1. Introduction 4
2. Policy Scope 4
3. Definitions 4
4. General Statement on Acceptable Use - Staff 4
5. File storage 5
6. Internet services 6
7. Mail services 6
8. Media rights 6
9. Security 7
10. Using social media 7
11. Teachers' Standards 7
12. Using a Personal Mobile Device for Work Purposes ("BYOD") 7
13. Use of artificial intelligence and external digital tools 8
14. Accessing Trust data off premises 9
15. Care of equipment 9
16. Data Protection 9
17. Computer security 9
18. Transferring data away from computer systems 10
19. Mobile devices 10
20. Reporting and Consequences of Non-Compliance 10
21. Policy Status 11
22. Related Policies 11

1. Introduction

1.1 This policy provides guidance on the acceptable use of IT equipment, systems, services and facilities within the David Ross Education Trust.

1.2 IT is seen as beneficial to all members of the Trust in supporting learning, teaching, research, administration and approved business activities of the Trust. The Academy's IT facilities provide a number of integral services and, therefore, any attempt to misuse a computer system could cause significant disruption to other users in the Trust. This could also lead to a breach of the data protection rights of individuals, resulting in harm to that individual and the Trust.

1.3 The Trust assumes the honesty and integrity of its IT users, including staff, contractors and consultants. The purpose of this policy is not to impose unnecessary restrictions, but to protect authorised users, pupils and the Trust from unlawful, unsafe or damaging actions, whether deliberate or accidental.

1.4 Facilities are provided for business use. The Trust may monitor, review and analyse use of its IT systems where necessary and proportionate for purposes including safeguarding, cyber security, data protection, regulatory compliance, business continuity, system maintenance and investigation of suspected misuse. Monitoring will be carried out in accordance with relevant legislation, this policy and the Staff Privacy Notice.

1.5 The Trust is bound in this regard by relevant legislation, including the UK GDPR, the Data Protection Act 2018, the Human Rights Act 1998, the Privacy and Electronic Communications Regulations 2003 and the Regulation of Investigatory Powers Act 2000.

2. Policy Scope

2.1 This policy applies to staff, contractors, trustees, members and governors within the Trust.

2.2 It is the responsibility of all individuals in the Trust to familiarise themselves with this policy and comply with its provisions.

3. Definitions

3.1 **Trust** means all academies within the David Ross Education Trust, as well as Central Support Services.

3.2 **Executive Leadership Team** means the Chief Executive Officer ("CEO") and the direct line management reports of the CEO (the "Directors").

3.3 **IT Facilities** means all IT devices, facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, audio-visual and connected devices, software, websites, web applications or services and any device, system or service which may become available in the future which is provided as part of the IT service.

3.4 **Users** means directors, members, trustees, governors, staff, students, trainees, volunteers, temporary guests, and all other persons authorised by the Trust to use the IT facilities.

3.5 **Personal use** means any use or activity not directly related to the users' employment, study or purpose.

3.6 **Materials** means files and data created using the IT facilities including but not limited to documents, photographs, audio, video, printed output, web pages, social networking sites, bulletin boards, newsgroups forums and blogs.

4. General Statement on Acceptable Use - Staff

4.1 The user agrees not to upload, download, post, email or otherwise transmit or store anything that:

- is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of anyone's privacy, hateful or racially, ethically or otherwise objectionable.
- the user does not have the right to transmit.
- infringes any patent, trademark, trade secret, copyright or other proprietary rights of any party.
- is unsolicited or unauthorised advertising, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes" etc.
- contains software viruses or any other computer code, files or programs designed to damage computer software, hardware or telecommunications equipment.

4.2 They also will not use the systems to:

- impersonate any person or entity
- interfere with or disrupt the service or servers or networks connected to the service, or disobey any requirements, procedures, policies or regulations of networks connected to the service.
- collect, store, use or disclose personal information about others except where this is necessary for authorised Trust purposes and is carried out in accordance with the UK GDPR, the Data Protection Act 2018 and Trust policies.
- undertake any trading, gambling, other action for personal financial gain, or political purposes unless as part of an agreed curriculum project.
- store or use any unauthorised software.
- use unapproved artificial intelligence, cloud, messaging or file-sharing tools to process Trust information, personal data, confidential information, pupil information or assessment material.

5. File storage

5.1 Files will be stored either on a Trust provided system with appropriate file-security, on a Trust approved network file store or, by prior agreement on a third-party system which meets the basic security requirements agreed by the Trust.

5.2 This includes the use of external USB storage of any kind which may not be used on any Trust IT system without previous written authorisation from the Director of IT and Data.

5.3 Files should never be stored on a public-access file store system not approved by the Trust. Any sensitive information to be emailed or otherwise transmitted outside the Trust must be encrypted to a standard agreed in advance with IT & Data team.

5.4 There are various cloud services in use by the Trust within the DRET.me system. Staff are required to only use those services that are supported by the Trust, secured by their business login (either @dret.co.uk or @academyname.co.uk) and have a relevant Data Sharing Agreement in place.

5.5 Trust email accounts should not be used to sign up or log in to services that are solely for personal use, such as personal shopping accounts or personal mailing lists.

5.6 It is not acceptable under any circumstances to use a personal cloud storage account (e.g. a personal Dropbox) to handle Trust data.

6. Internet services

6.1 The Trust expects users to act responsibly in accessing the internet and to report any offending material to the relevant authority.

6.2 As staff may access the internet through a number of public and private routes it is essential that staff use their professional judgment for their use of the internet.

6.3 Accessing inappropriate material over the internet, either using Trust equipment, or during working hours is a serious disciplinary matter.

6.4 All users should be aware that as well as monitoring internet traffic to block content, the Trust deems unacceptable; our systems also watch for keywords listed by the Home Office (as part of the PREVENT strategy) and the Internet Watch Foundation to raise an alert when a pattern of communication is one that may be a cause for concern.

6.5 Staff must report any safeguarding concern arising from internet use, online communication, filtering or monitoring alerts, AI-generated content, harmful content, attempted contact with pupils, or suspected online abuse through the academy's safeguarding procedures and to the Designated Safeguarding Lead without delay.

7. Mail services

7.1 Information held in a Trust administered email system is the property of the Trust.

7.2 All Trust staff that require email access as part of their duties will be provided with a business email address using the Trust approved service. The email address will either be @dret.co.uk or the recognised email domain of their academy (eg @cedarroadacademy.co.uk).

7.3 Personal email addresses must not be used to transact Trust business except in an emergency situation where a rapid response is required and the proper service is unavailable. When a personal address is used, a copy of the message must be sent to the relevant business address so that an audit trail is maintained.

7.4 Staff must maintain professional boundaries in all digital communication with pupils and families. Direct communication with pupils must only take place through Trust-approved systems and for a clear educational or safeguarding purpose. Personal email, personal messaging accounts and personal social media must not be used to communicate with pupils.

7.5 Emails of a confidential or sensitive nature must be clearly marked in the subject line so that the recipient is made aware. Sensitive or confidential information must only be shared using a Trust-approved secure method. Access should be limited to the intended recipients and additional protection, including encryption or a separate password, must be used where required by Trust guidance.

8. Media rights

8.1 Many files that can be purchased or rented privately, including music, films and streaming content, have licences that prohibit their storage, use or transmission on a business network.

8.2 Users must not use media they have purchased or rented on Trust systems unless they are certain that doing so complies with the relevant licence agreement.

8.3 Staff will not use personal accounts for viewing/streaming on Trust networks.

9. Security

9.1 Each user will be given a unique ID and password that will allow them to access their account. The ID and password are solely the responsibility of the user and not to be shared with other users or third parties for any reason.

9.2 All information about staff, pupils and other individuals will be handled in accordance with the UK GDPR, the Data Protection Act 2018 and Trust policies, and will only be shared where there is a lawful basis to do so.

9.3 The Trust reserves the right to monitor traffic, activity, emails and files on its network, either manually or through automated tools, where necessary and proportionate to support safeguarding, cyber security, data protection, compliance, business continuity, system maintenance and investigation of suspected misuse.

10. Using social media

10.1 When using social media, professionally or privately, staff must exercise professional judgement and ensure that content associated with them is consistent with their role and the Trust's values. Staff using social media for personal purposes should make clear that any views expressed are personal and must not use DRET email addresses, logos or other Trust branding unless authorised.

10.2 Contact with pupils through social media must not take place unless there is a clear, approved educational or safeguarding purpose agreed in advance by the Principal or headteacher and appropriate safeguards are in place.

11. Teachers' Standards

11.1 The 2011 Teachers' Standards apply in all respects for the use of IT by teaching staff. Teachers uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school, by:

- treating pupils with dignity, building relationships rooted in mutual respect, and at all times observing proper boundaries appropriate to a teacher's professional position
- having regard for the need to safeguard pupils' well-being, in accordance with statutory provisions
- showing tolerance of and respect for the rights of others
- not undermining fundamental British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs
- ensuring that personal beliefs are not expressed in ways which exploit pupils' vulnerability or might lead them to break the law. Teachers must have proper and professional regard for the ethos, policies and practices of the school in which they teach and maintain high standards in their own attendance and punctuality. Teachers must have an understanding of, and always act within, the statutory frameworks which set out their professional duties and responsibilities.

12. Using a Personal Mobile Device for Work Purposes ("BYOD")

12.1 All use of personal devices for work purposes is conditional on agreement to the following:

- If a computer, smartphone or tablet is connected to the Trust's IT systems, or holds information belonging to the Trust, it is covered by the same rules for Acceptable Use as the Trust's own equipment regardless of who it belongs to.

- The Trust takes no responsibility for the storage, maintenance or security of personal devices.
- Personal IT devices may not be used in any way that is disruptive or not conducive to a positive working environment.
- No effort may be made to bypass the security, filtering or monitoring arrangements put in place by the Trust. Any personal mobile device connected to Trust systems must be secured by a PIN, passcode, biometric protection or equivalent security measure, must have available security features enabled, and must be kept up to date with current security patches. Where appropriate, devices should be connected to Trust systems under the supervision or awareness of the IT Team. Any device that does not meet this criterion may be removed from Trust systems. Security settings and passwords may change at short notice and may require personal devices to be reconnected.
- The owner is responsible for making sure the device is safe to use.
- Some academies may only allow particular types of device on the system and their decision is final.
- The Trust has no responsibility for supporting any particular type of system. Technology changes and a new type of device may not be compatible with our services, or an older one may no longer be supported.
- The Trust reserves the right to withdraw access to its systems without notice.
- Any personal device used to hold any data belonging to the Trust (including emails) must be password or passcode protected (failure to do so would be misconduct).
- No confidential or personal data (including anything covered by Data Protection Policy) may be stored on a personal device at any time.
- On leaving the Trust, data related to employment with us may be automatically removed from the device.
- Cameras on personal devices must never be used to photograph or record students.
- If a personal device used for Trust purposes is lost, stolen, accessed by an unauthorised person or suspected to be compromised, the user must report this immediately to IT Support and follow the Trust's data breach reporting procedure where personal data may be affected.

13. Use of artificial intelligence and external digital tools

13.1 Staff must only use artificial intelligence, cloud services, collaboration platforms, apps or external digital tools for Trust business where the tool has been approved for that purpose by the Trust and appropriate information governance, data protection and safeguarding checks are in place.

13.2 Staff must not enter personal data, special category data, confidential Trust information, safeguarding information, pupil assessment information or unpublished Trust material into generative AI tools or other external platforms unless this has been expressly authorised and appropriate safeguards are in place.

13.3 AI-generated content must be checked carefully for accuracy, bias, confidentiality, copyright and safeguarding implications before it is used, shared or relied upon. Human professional judgement remains essential.

13.4 The IT & Data Team will maintain and publish guidance identifying approved tools and the

purposes for which they may be used. Where a tool is not listed, staff must seek approval before using it for Trust business.

14. Accessing Trust data off premises

14.1 When the Trust makes access to systems available offsite, the member of staff accepts responsibility for ensuring that nobody other than the authorised user gains access to the system, including by locking devices when unattended and avoiding use on shared or insecure devices.

15. Care of equipment

15.1 Equipment is provided for the purpose of carrying out your duties and must always be looked after with care.

15.2 Either at the end of the period of employment with the Trust, for servicing or for replacement, staff will be asked to return equipment.

15.3 The Trust reserves the right to charge the replacement cost of any lost items such as power supplies or cables that are required to reallocate the equipment to another user.

16. Data Protection

16.1 All staff are responsible for ensuring that they handle personal data with proper care and respect for the rights of colleagues, pupils, families and others, in accordance with the UK GDPR, the Data Protection Act 2018 and the Trust's Data Protection Policy.

17. Computer security

17.1 IT Support must ensure that all systems made available to staff use networks with appropriate firewall protection, virus checking must be installed on all computers and operating systems must be kept updated with security patches.

17.2 Staff have the responsibility not to tamper with or circumvent those systems and inform IT support if they believe their system is at risk.

17.3 Systems must be set up to allow staff access only to the personal information they need to do their job.

17.4 Staff should never share access to accounts and never share passwords. Where several people need to access a common account (e.g. an enquiries email address) it must be set up so that either one person monitors the account and informs colleagues, or as an alias where multiple members of staff receive communication from the shared address. It is the responsibility of the technical support and management staff in each academy to be aware of the potential for any kind of informal arrangement where passwords are shared and stop them.

17.5 Staff user accounts will be set upto multi-factor authentication (MFA) as directed by the Trust IT Team. MFA provides an added layer of security for Trust accounts and should be used for access to Trust-based systems wherever possible.

17.6 Users must enrol in and use multi-factor authentication wherever it is required or made available by the Trust and must not approve an authentication request they did not initiate.

17.7 In cases where an account falls dormant, either because someone has left employment with the Trust or is absent long-term, arrangements put in place must not compromise data security.

17.8 Any personal information held electronically that would cause damage or distress if it were lost or stolen must be encrypted (e.g. within a secure management information system or password protected file)

17.9 Local storage of computer systems used to retain any business data (e.g. computer hard disc) must be encrypted. Where an operating system is being used that does not support this as standard, a strong encryption alternative must be installed.

17.10 Regular back-ups of the information on computer systems must be taken and copies kept in a separate place. Under normal circumstances this is arranged by IT Support, however staff should ensure they are confident that important files are being backed up correctly. All information must be securely erased before disposing of old computers (through the use of secure erasure software or physical destruction of the hard disk).

18. Transferring data away from computer systems

18.1 Moving data between systems is one of the highest risk activities in terms of data protection and special care should always be exercised.

18.2 The preferred method for moving data is either through the use of the Trust email system, or the approved cloud storage systems within DRET.me.

18.3 External drives (such as USB pen drives) are not to be used and can only ever be used under the direct supervision of the IT Support team, who will ensure encryption is enabled, or with written permission from the Data Protection Officer, setting out the scope and limitations on use.

19. Mobile devices

19.1 Mobile devices also pose a security risk, in particular of “passive loss” of data where a colleague has a smartphone or tablet set up to receive business email or store files in some way

19.2 To minimise risk, any mobile device to be configured with a business email address must have a PIN lock enabled, if that is not possible then a business email address should not be used with that device. Staff must be aware that deliberately setting up access to their business email on an insecure device without taking steps to protect it is in breach of Trust Acceptable Use Policy

19.3 If a device holding Trust data (including email) is lost, Trust IT Support must be informed immediately to allow us to remotely wipe any sensitive data from the device.

19.4 Technical support staff in each academy will seek to authorise mobile devices on the Trust servers, so that if a device is lost or stolen it can be remotely wiped

20. Reporting and Consequences of Non-Compliance

20.1 Staff must report suspected or actual breaches of this policy promptly. This includes suspected data breaches, lost or stolen devices, suspected cyber incidents, phishing attempts, malware, inappropriate content, accidental misuse, unauthorised access, safeguarding concerns and any concern about the use of AI or external digital tools.

20.2 Reports should be made to the appropriate person or team without delay, normally IT Support

for technical or cyber-security matters, the Data Protection Officer for personal data incidents, the Designated Safeguarding Lead for safeguarding concerns, and the line manager or Principal/headteacher for conduct concerns.

20.3 Non-compliance with this policy may lead to disciplinary action being taken and, where appropriate, may also lead to withdrawal of access to Trust systems, referral to safeguarding procedures, data breach reporting or notification to external authorities.

21. Policy Status

21.1 This policy does not form part of any employee's contract of employment.

22. Related Policies

22.1 This policy is related to the following other Trust policies:

- Data Protection Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Disciplinary Policy
- Data Breach Procedure
- Online Safety Policy