David Ross Education Trust

Broadening Horizons

Acceptable Use Policy – Students

Document Management Information

Applicable to:	All students in all DRET academies. Parents and carers should be made aware of this policy and support students to follow it.
Dissemination:	The policy will be available to staff via the Trust's Policy Centre and to parents and students via the website.
Implementation:	Applicable to all DRET academies
Training:	On request
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	Version 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 January 2021
1. V1.2	Updated to clarify student scope, strengthen online safety, filtering and monitoring, personal device, AI and safeguarding expectations.	19 October 2026

Contents

Contents 3
1. Introduction 4
2. Policy Scope 4
3. Definitions 4
4. General Statement on Acceptable Use - Students 4
5. Internet Services 5
6. Security 5
7. Using Social Media 5
8. Care of Equipment 6
9. Reporting and Consequences of Non-Compliance 6
10. Related Policies 7

1. Introduction

1.1 This Policy provides the guidelines of acceptable use ofdigital technology and IT systems,facilities within The David Ross Education Trust.

1.2 Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and develop awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

1.3 This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

1.4 The Trust will provide students with access to digital technologies to support learning and will expect students to use those technologies safely, responsibly and respectfully. Use of Trust or academy systems may be monitored for safeguarding, security and appropriate use purposes.

1.5 The Trust will handle monitoring information in line with data protection law, safeguarding duties and relevant guidance. Monitoring is used to help keep students safe, protect Trust systems and respond to concerns.

1.6 The Trust filters and monitors the use of its systems to help keep students and the school community safe. Information from monitoring will only be accessed and used for appropriate purposes, including safeguarding, security and investigating suspected misuse.

2. Policy Scope

2.1 This policy applies to students within the Trust.

2.2 Staff are responsible for helping students understand and follow this policy, and for responding to concerns in line with safeguarding and behaviour procedures.

3. Definitions

3.1 **Trust** means all Academies within the David Ross Education Trust, as well as Head Office and central services operations.

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

4. General Statement on Acceptable Use - Students

4.1 You agree not to upload, download, post, email or otherwise transmit or store anything that:

- is unlawful, harmful, threatening, abusive, bullying, harassing, defamatory, hateful, discriminatory, obscene, invasive of privacy or otherwise inappropriate.
- you do not have the right to transmit.
- is "junk mail," "spam," "chain letters" or similar

- contains software viruses or any code designed to damage computer systems.

4.2 Students must not use Trust or academy systems to:

- impersonate any other person.
- interfere with or disrupt the IT service.
- collect or store personal information about other people.
- undertake any trading or 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 artificial intelligence tools in a way that is dishonest, unsafe, harmful or contrary to academy expectations, including presenting AI-generated work as their own without permission or acknowledgement.

5. Internet Services

5.1 Students must use the internet responsibly and report any harmful, inappropriate or worrying content to a member of staff immediately. Accessing, creating, sharing or attempting to bypass controls to access inappropriate material is a serious matter and may be dealt with under the academy's behaviour and safeguarding procedures. Internet use on Trust and academy systems is filtered and may be monitored to help protect students and the school community.

5.2 Students should not share personal information, images or videos of themselves or others unless this has been approved by staff and is safe and appropriate. Any concern about cyberbullying, online abuse, harmful contact, misinformation or unsafe online behaviour should be reported straight away.

5.3 Students must not photograph, video or audio-record another person without permission. Images and recordings must not be shared, altered or used to embarrass, impersonate, bully or harm another person.

5.4 Students must not create or share misleading, harmful or unauthorised AI-generated or digitally altered images, video, audio or impersonations of students, staff or other individuals.

6. Security

6.1 Students will be given a unique ID and password that will allow you to access your account. They are your responsibility and not to be shared with anyone for any reason.

6.2 You must use a secure password, must not approve another person's access to their account, and must tell a member of staff immediately if they think their password or account has been compromised.

7. Using Social Media

7.1 When using social media students should ensure that anything associated with them is consistent with their being a student at the school.

7.2 8. Use of Personal Mobile Devices and Bring Your Own Device ("BYOD")

7.3 Students may only use personal devices in school where this is permitted by the academy and in line with academy rules. There is no automatic right for students to use a personal phone, tablet, laptop or other device during the school day.

7.4 Where personal device use is allowed, students must follow all academy instructions and the following expectations:

- If your computer, smartphone or tablet is connected to the school's IT systems then it is covered by the same rules for Acceptable Use as the school's own equipment regardless of who it belongs to.
- The school takes no responsibility for storage, maintenance or security of your device.
- Personal devices must not be used in a way that disrupts learning, affects the wellbeing of others, breaches privacy or undermines a safe and respectful school environment.
- Students must not try to bypass Trust or academy security, filtering or monitoring arrangements.
- Where a personal device is permitted to connect to Trust systems or Wi-Fi, it must have a passcode or equivalent protection, be kept reasonably up to date and must not be used to bypass filtering, monitoring or other security controls.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 school 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 school reserves the right to withdraw access to its systems without notice.

8. Care of Equipment

8.1 Students must look after Trust, academy and personal equipment with care. Deliberate or careless damage may result in consequences in line with academy procedures and, where appropriate, the Trust may seek recovery of replacement or repair costs.

9. Reporting and Consequences of Non-Compliance

9.1 Any breach of this policy may result in action being taken in line with the academy's behaviour, safeguarding and IT procedures. Serious concerns may result in access to Trust systems being restricted or removed and, where necessary, concerns may be shared with parents, carers or external agencies.

9.2 Students should report any accidental access to inappropriate content, suspected cyberbullying, unsafe contact, security concern or loss of a device to a member of staff as soon as possible.

9.3 Students who accidentally access inappropriate or worrying content should close or minimise it where safe to do so and report it immediately. A student will not be treated as having deliberately breached the policy solely because the content was accessed accidentally and promptly reported.

10. Related Policies

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

- Data Protection Policy
- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Online Safety Policy