

Acceptable use Policy for Pupils

Document control			
Approved by	Full Trustees	Approved date	Feb 2026
Next Review		Policy Level	Non statutory
Published	Website & Intranet		
Version	Date issued	Author	Update information
V1.0	12/12/2017	N McDermott	First published version
V1.1	19/12/2019	N McDermott	Minor updates to aid reading ease. 2.2 Addition of invoice for damage caused clause.
V1.2	22/10/2020	N McDermott	Addition of key stroke monitoring to User Agreement s14.
V1.3	13 Jan 2021	N McDermott	Updated to reflect remote learning.
V1.4	2023	B Manning	
V1.5	February 2026	P Whittle	Addition of content around AI, misinformation, disinformation, and fake news.

Contents

1. Introduction.....	1
2. Aims	2
3. Pupil/Students Code of Conduct.....	3

1. Introduction

1.1. Dartmoor Multi Academy Trust recognises the value of technology in children's learning and development. There is also a sharp focus on the need to safeguard all children in respect of digital and online vulnerability. This policy should be read in conjunction with the most recent version of the Safeguarding & Child Protection Policy and Keeping Children Safe in Education (KCSiE), explains our expectations for how pupils are to use IT, both in schools and during remote learning. It will be reviewed annually.

- 1.2. As part of our curriculum, pupils have controlled, and appropriately filtered/monitored access, to the Internet and learn how to use libraries, databases and information sources on a wide variety of topics, as well as:
- Computers, laptops and other digital devices
 - The internet, which may include search engines and educational sites
 - School learning platforms e.g., Classcharts, Google Classroom, Microsoft Team, Class Dojo.
 - Email
 - Games consoles and other games-based technologies
 - Digital cameras, webcams and video cameras

1.3. Other policies (accessible on our website [here](#)) that are related to this policy include:

- Schools' Behaviour Policies (see individual school websites)
- Social Media Policy
- Safeguarding & Child Protection Policy
- Data Protection
- Online Safety Policy
- Code of Conduct for Parents Carers and Visitors
- Code of Conduct and Online Media Use Statement for Students, Parents/Carers and Visitors
- Mobile Phone Policy
- Personal, Social & Health Education (PSHE) Policy
- Relationships Sex Education (RSE) Policy.
- AI policy

2. Aims

2.1. The Trust will support pupils to be safe and responsible users of technology and:

- Become empowered and responsible digital creators and users.
- Use resources and technology safely, carefully and responsibly, respecting system security and password security.
- Be kind online and help create a community that is respectful and caring, on and offline.
- Be safe and sensible online and always know that they can talk to a trusted adult if they are unsure or need help.

2.2. **We value safe behaviour.** All activity carried out using Trust systems and hardware is subject to filtering and therefore control of content and, in the case of keyboard enabled devices, monitoring both through the use of a keystroke based detection system; "Smoothwall" and adult vigilance and observation. Any misuse of technology will be dealt with according to our schools' Behaviour and Anti-Bullying policies. This can include:

- deliberately uploading or adding any images, video, sounds or text that could upset, offend or threaten the safety of a member of the school community.
- misuse or damage to school equipment. An invoice may be raised to cover the cost of repair or replacement of the damaged equipment.
- using technology without permission and at times that are not allowed.
- bypassing school filtering and monitoring systems (this includes, but is not limited to, the use of VPN, personal hotspot devices, attempting to change school computer settings, using portable apps and anonymous browsers).

2.3. **We recognise there are potential risks.** The Trust will take all reasonable precautions including regular staff training and monitoring and filtering systems (supervised by Designated Safeguarding personnel), to ensure that pupils and staff are as safe as possible when using school equipment, our internet and systems. This monitoring will

be proportionate and will take place in accordance with Keeping Children Safe in Education (KCSiE), data protection (including GDPR), privacy and human rights legislation. The Trust reserves the right to monitor the activity of all users on school systems. We will refer to [Saferinternet.org.uk](https://saferinternet.org.uk) provider self-certification when selecting providers to ensure they meet appropriate safety standards.

- 2.4. We recognise that the internet is constantly changing**, with new apps, devices, websites and AI material emerging at a rapid pace. We will regularly review the methods used to identify, assess and minimise online risks, as well as examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is allowed. Online harms include misinformation, disinformation, fake news, and conspiracy theories, alongside existing risks like extremism and bullying. Pupils need support to recognise and challenge misleading information online, and are taught to employ critical thinking strategies.
- 2.5. We recognise that no technical system can replace online safety education.** We will:
- embed online safety education in curriculum delivery, wherever possible.
 - model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
 - develop awareness of E-safety issues through regular training and curriculum delivery.
 - take appropriate action where necessary.
- 2.6. All pupils and parents have an important role to play in developing responsible behaviour.** We will share the messages in this policy with pupils in school and encourage parents to read and discuss the key points with their children at home. We ask parents/carers to role model safe and positive online behaviour and discuss online safety at home. Links to extra resources and help is on our website <https://www.dartmoormat.org.uk/online-safety.html>
- 2.7. Some pupils may be more vulnerable online.** This may include children in care, children with special educational needs and disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. We will ensure that differentiated and appropriate online safety education, access, and support is provided to vulnerable pupils and seek input from specialist staff as appropriate, including the SENDCO, Inclusion Lead(s) and Children in Care Lead.
- 2.8. We respect the law.** If we believe a pupil has committed a criminal offence, we will contact the relevant authorities. School owned information systems, including Wi-Fi, must be used lawfully. The Computer Misuse Act 1990 states the following criminal offences:
- 2.8.1. to gain unauthorised access to computer material.
 - 2.8.2. to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. Pupil/Students Code of Conduct

1. I will only use school/college ICT systems, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes, whether I am in school or not.

2. I will not engage in any form of cyber bullying.
3. I will follow all instructions issued by my teacher and use technology as they direct me to do.
4. I will only log on to the school network/ Learning Platform with my school provided username and password. I will never share my username or password with anyone else.
5. I will always log off properly when I have finished using school systems/platforms.
6. I will not download or install software on school technologies or use USB flash drives/ memory sticks on school hardware.
7. I will only use my school/college e-mail address for school related things including contacting my teacher.
8. I will not attempt to bypass any computer or user account restrictions to access confidential or otherwise restricted information on the school/college network.
9. I will not try to bypass the internet filtering systems in school/college.
10. I will make sure that all electronic communications with pupils, teachers or others are responsible and sensible.
11. I will be responsible for my behaviour when using school/college platforms. This includes resources I access and the language I use.
12. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
13. I will ensure that my online activity, both in school and outside school/college, will not cause my school, the staff, pupils or others distress or bring them into disrepute.
14. I will follow the school/college approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school/college community.
15. I will respect the privacy and ownership of others' work on-line at all times.
16. I understand that in school/college, all my use of the internet, keystrokes on school devices and other related technologies may be filtered, monitored, logged and made available to teachers, to protect me and others and the integrity of school systems.
17. I understand that these rules are designed to keep me safe and that if they are not followed, school/college sanctions will be applied, and my parent/ carer will be contacted.

For remote learning:

18. I will have my camera switched on and microphone muted at the start of any 'live' sessions.
19. I will use a blurred background or a 'backdrop' image.

20. I will promptly log in to any 'live' session at the time it is scheduled to start.
21. I understand that 'live' sessions may be recorded by the school and may be made available for students to access later, for educational and safeguarding (including behaviour) purposes only and will be stored for no longer than 28 days.
22. I will dress appropriately for all 'live' sessions.
23. I will not record or take photos of my teachers or classmates, or any lesson content.
24. I understand that to make the most out of any 'live' session I should ensure that:
 - I am in a quiet, safe and appropriate environment with minimal distractions.
 - Use headphones for lessons, wherever possible.
 - I am attentive and follow all instructions, treating others with respect particularly where technical issues cause disruption to your learning.

Parents and carers should support pupils/students and teachers by:

1. Discussing the above rules and expectations with their child.
2. Providing their child with a workspace that is quiet, safe and free from distractions.
3. Making sure that their child is dressed appropriately (school uniform is not necessary).
4. Ensuring that face-to-face communication is only between teachers and students, i.e. any parent-to-teacher communication should be in the usual manner.

Parents and carers must:

5. Not record any part of a lesson and should refrain from commenting on public forums about individual teachers.
6. Be aware that online lessons may be recorded for educational, safeguarding (including behaviour) purposes and will be stored for no longer than 28 days.