



Midsomer Norton Schools Partnership

Issued: January 2026
Review: Term 1 annually
LST: MLY

ICT ACCEPTABLE USE POLICY (Pupils)

Our Acceptable Use Agreement

1) The Aims of this policy

- a) This Acceptable Use Policy provides pupils with the guidelines and instructions on how to use ICT within the Midsomer Norton Schools Partnership Trust (known as the Trust) and is applicable to all schools. All pupils are entitled to access the school ICT systems.
- b) The Student AUP is aimed to ensure that pupils can use the school ICT systems - Internet, Email, Cloud services and other technologies available such as mobile devices, tablets and ChromeBooks, both at the school and externally - in a safe and secure way.
- c) Parents/Carers play a crucial role in ensuring that pupils understand the need to use ICT in a safe and responsible way. Schools will provide ICT guidance and updates to parents/carers when applicable. Parents/carers have a responsibility to monitor their child's use of technology to support the school in promoting good e-safety practice and to follow the guidelines outlined in this policy.

2) The Agreement

- a) By enrolling at a Midsomer Norton Schools Partnership school, pupils and parents/carers agree to the terms of this Acceptable Use Policy.
- b) This policy and agreement extends to all hardware and software provided by the school. Including but not limited to: PCs, laptops, tablets, webcams, whiteboards, digital video equipment and technologies owned by pupils that have been brought onto the school premises.
- c) Breaches of the agreement can result in a ban from the use of the ICT facilities and include confiscation of devices. Further action can be taken under the Trust's behaviour procedures and policy breaches may also lead to criminal or civil proceedings. Users of the ICT systems may be held liable for costs incurred for repair and/or replacement of equipment where the damage was caused by misuse.

3) Equipment

- a) All Trust computing equipment must be treated with care and respect.
- b) Pupils are prohibited from moving electronic equipment and must seek professional guidance before attempting to operate any unfamiliar equipment.
- c) Any identified damage or malfunction must be reported to a member of staff immediately.
- d) USB devices are not permitted except under the direction of a teacher.

4) Security

- a) Pupils must not use another person's account and must lock their screen when unattended.
- b) If a security issue is identified a member of staff must be notified immediately.

5) Passwords

- a) Passwords are strictly private and must not be shared with others.
- b) The IT Support Team will re-set passwords which are insecure, and reserve the right to suspend the account
- c) Passwords should be strong with a combination of letters, numbers, and special characters. For help with creating strong passwords click [here](#) (National Cyber Security Centre).
- d) Passwords should not be reused across other platforms/systems.

6) Email

- a) Pupils are responsible for all correspondence sent from their accounts and are expected to check their school email at least once daily during term time.

- b) Pupils must not open attachments, click links, or reply to unexpected emails. Replying to spam, forwarding chain letters, or sending unsolicited mass emails is strictly prohibited. Such messages should be deleted immediately and reported to IT Support to prevent further network disruption.
- c) The use of school or personal email during lessons is permitted only when explicitly authorised by the teacher for educational purposes.

7) Use of Artificial Intelligence (AI) - to be read in conjunction with the AI policy.

- a) Unless directed by their teachers, pupils and pupils may not use AI for classwork.
- b) Where pupils are permitted to use AI, pupils must use the Trust's Google AI solutions that are linked to the users Trust account. This version of AI has been certified as being suitable in an education environment, although all AI should be used with caution.
- c) Pupils must not put any personal information into AI systems
- d) At KS4 and KS5, pupils following exam courses must adhere to all JCQ regulations relating to the use of AI in elements of external assessments.

8) Educational Purpose

- a) The computer systems (including networks and cloud environments) within the Trust have been established for educational purposes.
- b) Pupils may use the ICT systems for limited personal use in wrap-around care with permission from a staff member and in strict adherence to the 'Acceptable Use Policy' outlined in this document.

9) Plagiarism and Copyright

- a) Plagiarism is taking the ideas or writings of others and presenting them as your own.
- b) Pupils must not plagiarise work that is found on the Internet or anywhere else and respect copyright.
- c) Sources must be referenced when producing work via footnotes or bibliographies.

10) Personal Safety

To ensure the safety and wellbeing of all users, pupils must adhere to the following safeguarding principles:

- a) Users must exercise caution regarding their personal information. Private information such as addresses, email addresses and phone numbers should never be disclosed to strangers or shared on public platforms.
- b) Pupils must never arrange to meet anyone they have met online, as digital identities can be easily falsified. It is essential to remain authentic online and avoid misrepresenting one's identity or intentions.
- c) If a student encounters inappropriate language, uncomfortable content, or suspicious contact they must inform a staff member immediately.
- d) If a user is ever in doubt about the safety of an online activity or the legitimacy of a contact, they should consult a staff member before proceeding.

11) Software

- a) Pupils must not install any software or programmes on the school systems.

12) Printing

- a) Printing is available in all schools where necessary; it is expected that printing will be minimal. Additional requests can be made via the local IT team.
- b) Where pupils are unable to act responsibly when using the printing services, their use of these facilities will be removed.

13) Privacy & The Right to Monitor

- a) All files and emails provided by the school are the property of the Trust. As such, staff have the right to access if required.
- b) All network access, web browsing and emails on the school system are logged, and filters are in place to restrict inappropriate websites being accessed (see Internet Filtering Policy).
- c) The Trust reserves the right to randomly search the Internet for inappropriate material posted by pupils and act upon it. This includes, but is not limited to, searching social media websites for inappropriate content posted about schools or persons within the Trust. Any inappropriate use is a violation of this AUP. Any individual found to be in violation of this AUP will be subject to disciplinary action in line with the School's Behaviour Policy.

14) Improper Use

- a) Examples of improper use by pupils includes but is not limited to:
 - i) Malicious damage of computing equipment
 - ii) Persistent attempts to circumvent the ICT systems security;
 - iii) Cyber-Bullying

- iv) Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- v) Activity which defames or disparages the school, or risks bringing the school into disrepute
- vi) Using inappropriate or offensive language
- vii) Downloading materials or images not relevant to their studies
- b) If ICT is used in an improper way sanctions will be given in line with the schools behaviour policy which may include but is not limited to parents/carers being notified, suspension of the user account, detentions and/or suspensions. Where the misuse is in contravention of UK law, the school may also need to disclose the incident to authorities outside of the school.

15) Examining electronic devices

- a) The Headteacher, and any member of staff authorised to do so, can conduct a search and confiscate personal electronic devices if they have reasonable grounds for suspecting the device:
 - i) poses a risk to staff or pupils,
 - ii) could undermine the environment of the school
 - iii) could cause disruption to the learning of other pupils
 - iv) is evidence related to an offence or is being used for a criminal activity, in which case it will be handed directly to the relevant authorities. Where a device is suspected of holding indecent images, the device will be confiscated and handed to the relevant authorities; the school will not review the images

16) Account De-provisioning

- a) Student accounts will transfer between schools if applicable.
- b) Accounts will be deleted once they have left the Trust.
- c) Pupils in Year 11 and Year 13 will have access to their accounts for 1 month after exam results, after that time the accounts will be deleted (Y11 accounts will not be deleted if they are continuing to KS5).

17) Bring Your Own Devices (BYOD)

- a) The use of your own IT equipment at school is encouraged to support your learning and educational journey/experience.
- b) To support this the Schools within the Trust have created a separate WiFi network to allow pupils to connect personal devices to the internet without seeking prior approval. This WiFi network will be visible on your internet enabled device. If you decide to connect your device to this network you are still using school facilities and are still bound by the other items in this Acceptable Use Policy. You should also be aware of the following:
 - i) When you connect a device to this network you should mark it as a 'public' network as this will help protect your files from other activity on this network. If you make your computer visible to others you are more at risk of having files used, altered or deleted by others.
 - ii) Under no circumstances should you attempt to access files on another user's computer. Pupils should disable sharing of any 'media' i.e. iTunes libraries, as this is way in which you may be breaking copyright law. If you are unsure of how to disable this, please visit the IT office for assistance.
 - iii) Pupils should not use the BYOD network to enable collaborative gaming, this is often network intensive and may have a detrimental effect on the performance of the network, thus impacting genuine academic users.
 - iv) Pupils are encouraged to run the latest operating system (iOS on Apple) and apply current updates to their device to ensure the latest security updates/patches are applied.