Digital Device, Online Safety and Responsible Use Policy 2026–2027

Implemented:	**September 2021**
Next Review:	**June 2027**

1. Purpose and Rationale

This policy sets out The Winchester School's expectations for the safe, responsible, ethical and purposeful use of digital devices, school networks, online platforms, artificial intelligence tools and other digital technologies. It supports high-quality teaching and learning, protects students from online harm, promotes digital citizenship and ensures that all users understand their responsibilities when using technology in school, at home or in any context connected to the school.

2. Scope

This policy applies to all students, parents and guardians, staff, visitors and any other users who access school networks, systems, devices, applications, online platforms or digital services. It applies to school-owned devices, personal devices used under the Bring Your Own Device arrangement, mobile phones, tablets, laptops, smart devices, wearable technology, online accounts, email, learning platforms, cloud storage, artificial intelligence tools and any future digital technologies used for school-related purposes.

3. Aims of the Policy

- To ensure that technology is used safely, responsibly and effectively to enhance learning.
- To protect students from online risks, including harmful content, unsafe contact, cyberbullying, exploitation, scams, misinformation and misuse of emerging technologies.
- To promote respectful digital behaviour, digital wellbeing and positive online reputation.
- To provide clear expectations for BYOD, mobile phones, online communication, data protection, cybersecurity and artificial intelligence.
- To ensure that students, parents and staff understand how to report concerns and how the school will respond to misuse.
- To align digital practice with school safeguarding, behaviour, data protection and child protection procedures.

4. Key Definitions

- **Digital device:** Any device capable of accessing, storing, creating or sharing digital content, including laptops, tablets, mobile phones, smartwatches, cameras and wearable technology.
- **BYOD:** Bring Your Own Device, where students use an approved personal device for learning under school expectations.
- **School network:** The school's Wi-Fi, internet connection, servers, platforms, systems and related digital services.

- **Online safety:** The protection of students and users from risks that arise through digital technology and online interaction.
- **Cyberbullying:** Bullying or harmful behaviour carried out through digital devices, online platforms, messages, images, videos or social media.
- **Artificial intelligence:** Digital tools that can generate, analyse or adapt content, including text, images, audio, video or data.
- **Personal data:** Any information that can identify an individual, including names, photographs, contact details, school records, usernames or account information.

5. BYOD and Digital Device Expectations

- Students must register personal devices with the School IT Department before connecting them to the school Wi-Fi network or using them on campus.
- Only one approved BYOD device per student may be connected to the school Wi-Fi network.
- Students may bring laptops or tablets that do not contain SIM cards, 4G/5G data packages or independent mobile data access.
- Students must use only the school-provided internet connection while on campus and must not use hotspots, tethering or external wireless connections.
- Devices must be used only for educational purposes and only when directed or permitted by a teacher.
- Devices must be fully charged, clearly labelled, kept secure and used in silent mode unless sound is required for learning and approved by the teacher.
- Students remain responsible for the safe care, storage and transport of their personal devices. The school is not financially responsible for loss, theft or damage to personal devices.
- Printing from personal devices is not available.
- Devices must not be used during assessments unless explicitly permitted by the teacher as part of approved access arrangements or assessment requirements.

6. Mobile Phone Expectations

- Students are not permitted to use mobile phones or communication-enabled smart devices at any time during the school day, including during lessons, break and lunch times, school activities, trips and events, or while remaining on campus after school.
- Where a phone is brought to school for travel or communication after school, it must remain switched off and securely stored in the student's bag or locker throughout the school day. Should a student need to contact home, this must be done through the School Reception or Office. Parents requiring urgent contact with their child are similarly requested to contact the school directly.

Stepped Response for Non-Compliance

First Incident: Written Warning

- The device will be confiscated immediately and securely stored in the School Office.
- Parents will be informed and the incident will be recorded and a written warning issued.
- The device will be returned at the end of the school day.

Second Incident: Parent Collection

- The device will be confiscated and securely retained by the school.
- The incident will be recorded as a repeated breach.
- Parent/guardian attendance will be required and the device will only be released to the parent/guardian.
- The matter will be addressed in accordance with the School Behaviour Policy.

Third Incident: Final Warning and Formal Escalation

- The device will be confiscated and a final written warning issued.
- Parent/guardian attendance will be required and the device will only be released to the parent/guardian.
- The matter will be formally escalated in accordance with the School Behaviour Policy.
- Where the nature of the incident meets applicable UAE reporting requirements, it may be referred to the relevant authorities.
- **Serious misuse is considered red-line behaviour and may be escalated immediately, irrespective of whether it is a first incident.** This includes unauthorised filming, photography or recording; cyberbullying; inappropriate or harmful content; breaches of privacy; safeguarding concerns; or conduct that may be unlawful or culturally insensitive and inappropriate.

7. Acceptable Use of Technology

- Use digital devices, school systems and online platforms to support learning, research, collaboration and school-approved activities.
- Follow teacher instructions and use only approved applications, websites, files and learning platforms.
- Communicate respectfully, professionally and appropriately in all online interactions.
- Respect the rights, privacy, dignity and wellbeing of others.
- Respect copyright, intellectual property and licensing requirements, and acknowledge sources appropriately.
- Use school accounts, subscriptions and files only for authorised school purposes.
- Maintain the security and integrity of school networks, devices and systems.
- Use technology in a way that reflects the school's values and UAE expectations for responsible conduct.

8. Unacceptable Use and Prohibited Behaviour

- Accessing, creating, storing, downloading, transmitting or sharing inappropriate, unsafe, offensive, discriminatory, extremist, violent, harmful or illegal content.
- Cyberbullying, harassment, intimidation, impersonation, exclusion, trolling, abuse or any other harmful online conduct.
- Using another person's account, password, files, subscription, device or personal information.
- Sharing passwords, usernames, one-time passcodes or confidential information.
- Attempting to bypass, disable or interfere with filtering, monitoring, firewalls, security settings or school network controls.

- Downloading, installing or using unauthorised software, games, applications, hidden files or programmes.
- Introducing viruses, malware or any programme designed to damage, alter, destroy or provide unauthorised access to systems or data.
- Photographing, filming, recording or sharing images, videos or audio of staff, students, parents or visitors without explicit permission and school approval.
- Using personal messaging, email or social media to communicate during the school day unless approved for a school purpose.
- Using technology to damage the reputation of another person, the school or the wider community.
- Any use that breaches school policy, UAE law, safeguarding expectations or the school's standards of behaviour.

9. Online Safety and Digital Safeguarding

The school is committed to safeguarding students online as well as offline. Digital safeguarding is the responsibility of all members of the school community. Students must report any online concern immediately to a trusted adult, teacher, pastoral leader, Designated Safeguarding Lead, parent or member of the IT team.

- **Content risks:** Exposure to harmful, inappropriate, extremist, violent, misleading, discriminatory or age-inappropriate material.
- **Contact risks:** Unsafe communication, grooming, impersonation, peer pressure, exploitation or contact from unknown individuals.
- **Conduct risks:** Cyberbullying, harassment, sharing harmful content, misuse of images, unsafe online behaviour or harmful digital choices.
- **Commerce risks:** Phishing, scams, online fraud, gambling, in-app purchases, targeted advertising or financial exploitation.
- **Privacy risks:** Sharing personal data, weak passwords, identity theft, misuse of accounts, deepfakes or unauthorised use of artificial intelligence.

10. Social Media,Digital Citizenship and Online Reputation

- Students must not photograph, film, record, upload, distribute or share images, videos or audio of others without permission and school approval.
- Images, recordings or social media posts must never be used to bully, shame, embarrass, threaten, impersonate or harm another person.
- Students must respect platform age restrictions and terms of service.
- Students should understand that digital content may remain online permanently and may affect future educational, professional and personal opportunities.
- Staff and students must use only school-approved communication channels for school-related communication.
- Students must follow UAE rules and regulations regarding use of social media.

- Students are expected to act as responsible digital citizens. Before posting, commenting, sharing or forwarding content, students should apply the THINK principle, Is it?
  T: True,
  H: Helpful,
  I: Inspiring,
  N: Necessary
  K: Kind
- Students should contribute positively to online communities, avoid plagiarism, respect copyright and recognise that their digital footprint forms part of their personal reputation.

11. Cybersecurity, Data Protection and Privacy

- Users must keep passwords, usernames, account details and one-time passcodes confidential.
- Users must log out of accounts and devices when they are no longer in use.
- Users must avoid opening suspicious links, attachments, emails, messages or downloads.
- Users must keep devices secure, updated and protected from malware where possible.
- Users must not share personal, confidential or sensitive information unless authorised to do so.
- Any suspected data breach, data loss, cyber threat, account misuse or unusual digital activity must be reported immediately.
- The school may inspect, review or restrict access to devices, accounts or systems where there is safeguarding, cybersecurity, behaviour or compliance concern.

12. Artificial Intelligence and Emerging Technologies

- Students may use approved artificial intelligence tools only when authorised by a teacher and only for the intended learning purpose.
- Students must acknowledge the use of artificial intelligence where required by the teacher or assessment guidance.
- Students must not use artificial intelligence to misrepresent work, gain an unfair academic advantage, create harmful content or impersonate others.
- Students must critically check artificial intelligence outputs for accuracy, bias, reliability and appropriateness.
- Students must not upload personal, confidential, sensitive or school-protected information to artificial intelligence platforms unless explicitly authorised.
- Any harmful, misleading, discriminatory, unsafe or concerning artificial intelligence-generated material must be reported immediately.

14. Monitoring and Filtering

- The school operates monitoring and filtering systems to provide a safe online environment, protect students from harmful or inappropriate content, support safeguarding and maintain the security of school systems.
- Filtering helps prevent access to inappropriate material, while monitoring supports the identification and response to concerning or unsafe activity.
- Users should have no expectation of privacy when using school networks, school systems, school devices or school-managed digital services.

15. Parents Responsibilities

- Monitor and supervise their child's use of digital devices, online platforms, applications and websites.
- Regularly review the content their child is accessing, including videos, social media content, online games and websites, to ensure it is age-appropriate and aligns with family and school values.
- Ensure that children do not share passwords, usernames, one-time passcodes (OTP), or personal account credentials with friends or other individuals.
- Encourage the use of strong passwords and support children in maintaining the security of their online accounts.
- Monitor and manage their child's social media use and ensure that privacy settings are appropriately configured.
- Recognise that most social media platforms have minimum age requirements and ensure compliance with these age restrictions. As per UAE law, students below the age of 15 should not operate personal social media accounts without active parental supervision and consideration of platform age restrictions.
- Discuss online safety regularly with their child, including:
    - Cyberbullying
    - Online grooming
    - Online scams and phishing
    - Inappropriate content
    - Digital footprints and online reputation
    - Safe and responsible use of Artificial Intelligence (AI)
- Encourage open communication so that children feel comfortable reporting any online concern, inappropriate communication, or digital safeguarding issue.
- Inform the school immediately if their child experiences or discloses:
    - Cyberbullying
    - Online harassment
    - Online grooming
    - Exposure to harmful or inappropriate content
    - Youth-produced sexual imagery (YPSI)
    - Online scams or digital security concerns
    - Misuse of AI or other emerging technologies

- Ensure that devices used by students have appropriate parental controls, content filtering and security settings where possible.
- Support the school's Digital Device Responsible Use Agreement (DDRUA), Online Safety Policy and Safeguarding Policy.
- Reinforce responsible digital citizenship by encouraging respectful online behaviour and modelling positive use of technology.
- Ensure that students understand that information posted online may remain permanently accessible and may impact future educational, professional and personal opportunities.
- Work collaboratively with the school to address any concerns relating to online behaviour, digital wellbeing, safeguarding or misuse of technology.
- Promote healthy screen time habits and encourage a balanced lifestyle that includes physical activity, social interaction and wellbeing.
- Always maintain respectful communication
- Use approved educational platforms only
- Ensure your child does not access any online platform using another student's credentials.

16. Reporting Concerns and Incident Response

- All concerns relating to online safety, digital behaviour, device misuse, cybersecurity, data protection or safeguarding must be reported immediately to a teacher, pastoral leader, Designated Safeguarding Lead, member of the Senior Leadership Team or IT Department as appropriate.
- Reports will be taken seriously, recorded where required, investigated in accordance with school procedures and escalated to parents, safeguarding agencies or external authorities where necessary.

17. Consequences of Misuse

- Temporary or permanent withdrawal of device, network or platform access.
- Confiscation of mobile phones or devices where misuse occurs.
- Parent meeting, behaviour reflection, restorative action or behaviour contract.
- Sanctions in line with the school Behaviour Policy.
- Safeguarding intervention and support where appropriate.
- Referral to external agencies or authorities where behaviour is unlawful, harmful or presents a safeguarding risk.

18. Linked Policies and Guidance

- Safeguarding and Child Protection Policy
- Behaviour And Discipline Policy
- Anti-Bullying Policy
- Teaching and Learning Policy
- Assessment Policy
- IT and Cybersecurity Procedures

19. Student and Parent/Guardian Agreement

By signing this agreement, the students and parent/guardian confirm that they have read, understood and agreed to follow The Winchester School Digital Device, Online Safety and Responsible Use Policy. They understand that misuse of technology may result in loss of digital privileges, behaviour sanctions, safeguarding action or referral to relevant authorities where necessary.

Signed : Meenakshi

Date : June 2025

Digital Devices Acceptable Use Agreement

As a student at The Winchester School, I acknowledge that I have read through and agree to The Winchester School Digital Device, Online Safety and Responsible Use Policy and agreement.

Full name of Student ……..

Year Group and Section ……

Date ……..

Signature of Student ……..

Signature of Parent ……

I acknowledge that my son/daughter and I have read through and agree to The Winchester School Digital Devices Acceptable Uses Agreement. I will instruct my child regarding the importance of following all the guideline included in this agreement.

I understand that any violation will result in the loss of technology privileges as well as other disciplinary action.

Signed :
Date : June 2026