Digital Technology Acceptable Use Policy

The Cottesloe School

Policy Type:	Non Statutory
Reviewed by:	Simon Clawson (Strategic Digital Lead), Mark Watson (Link Governor) and Mr S Jones (Headteacher)
Date:	Summer Term 2026
Approved by:	Teaching and Learning - June 2026
Next review:	Summer Term 2028

Contents

Introduction

This policy outlines the acceptable use of digital technology by staff and students at The Cottesloe School. It applies to all school-owned devices, networks, internet access, and online platforms, as well as personal devices used on school premises or for school-related activities, both now and in the future. The policy aims to ensure safe, legal, responsible, and effective use of technology for learning, teaching, and administration, while safeguarding the well-being of our community. By working together, we can create a positive and productive learning environment for all.

1. Scope

This policy covers:

- All school-owned devices (e.g., Chromebooks, laptops, desktops, tablets, interactive whiteboards).
- The school's network, internet access, and online platforms.
- Personal devices (e.g., smartphones, laptops, tablets) used on school premises or for school-related activities.
- Social media and online platform use by staff in relation to their professional role, including but not limited to:
    - Promoting the school and its activities
    - Communicating with parents and students
    - Sharing educational resources and best practices
    - Networking with other professionals
    - Participating in online professional development
    - Using social media for research and lesson planning
    - Engaging in online discussions and debates related to education
    - Using social media to support student learning and engagement
- Emerging technologies and their potential use within the school environment including, but not limited to Artificial Intelligence (AI), online learning tools, assessment platforms and other interactive learning services.

2. Staff Use of Digital Technology

For the purposes of this policy, staff refers to all adult users on The Cottesloe School computer network, in any capacity, who have login access or connections to the school wifi network or other systems, including, but not limited to, teachers, agency personnel, contractors, exam invigilators, volunteers and governors.

Staff are encouraged to use technology to be creative and innovative in their teaching and to support their duties. While this can bring a wide range of advantages it should be used with care and consideration for data privacy and cybersecurity. All devices that use school data must be locked when left unattended to prevent unauthorised access.

2.1 School-Owned Devices:

- School-owned devices are provided for school-related work only. They should not be used to perform tasks for any other organisation or employment.
- Staff are responsible for the security and proper care of assigned devices. Staff must take all reasonable precautions to ensure the safety and security of school property when off-site. Devices must not be left unattended in vehicles. All issues with school related devices should be reported to the IT manager, using SpiceWorks.
- Software installation requires prior approval from the IT manager. All installed software must be assessed to ensure any data it uses is properly managed as per the school GDPR policy.
- Staff must not attempt to bypass security measures such as firewalls or content filters to intentionally access inappropriate content. Inappropriate content includes, but is not limited to, pornography, violent content, hate speech, material promoting illegal activities, and content that could be considered bullying or harassment.
- Staff must not share their login information with anyone else under any circumstances. Any suspicion that login details have become known to anyone other than the user should be reported to the IT Manager and the affected account should have a password change carried out.

2.2 Personal Devices:

- We do not encourage the use of personal devices in school for staff. For both well-being and GDPR reasons it can create extra issues and risks. However we do understand that there may be a need to use a device such as a laptop or personal Chromebook at times. Where possible please use a school desktop device or Chromebook for any in-school tasks.
- Staff personal mobile devices should not be used in lessons or in view of students. The use of headphones and other devices should be restricted to non teaching areas only.
- Personal devices used for school work must be protected by a strong password (the school recommends the NCSC 'three random words' strategy) or biometric lock, and enabled device encryption. Staff must ensure that any installed software is up to date to maintain security within the school network.
- The school is not responsible for the loss or damage of personal devices.
- Staff must ensure that any school data stored on personal devices is securely stored within the school Google Drive cloud storage, and deleted when no longer required.
- Loss of a personal device that may contain school data, for example a mobile phone that is logged into Google Mail, should be reported to the Data Protection Lead as soon as possible.
- Personal devices must not be used to record or photograph students. If any images of work or other materials can be used to identify students they should be transferred to school storage and removed from the personal device as soon as possible.
- External storage devices are blocked for general use. Where required they may be unlocked on specific systems, must be asset tagged and must be checked, prior to use, with antivirus software. All data held on external devices must be encrypted to protect against unauthorised access.

2.3 Social Media:

- Staff must maintain professional conduct on social media platforms, even in personal accounts, when their connection to the school is identifiable. Staff should not include their school employment details in their personal social media profiles. This expectation of professional conduct extends to personal online behavior that could reasonably be associated with the school. Examples of unacceptable behavior include:
    - Sharing or endorsing discriminatory or hateful content.
    - Publicly criticizing the school, staff, or students and their families.
    - Posting content that violates the school's safeguarding policies.
- Posts representing The Cottesloe School must adhere to the branding guidelines, photo permissions and any guidelines regarding sharing of personal information. All posts should be made using the official school accounts and should be proofread carefully before posting. Posts representing official school announcements or policy should be approved by Senior Leadership
- More details can be found in The Cottesloe School Staff Code of Conduct.

2.4 Safeguarding:

- Staff and students are prohibited from connecting on personal social media accounts, unless a pre-existing familial relationship exists.
- This includes "friending," "following," direct messaging, and other forms of online interaction including gaming and other broadcasting methods. Any existing online connections must be declared to the Headteacher.
- Where a professional account such as LinkedIn is used, staff should ensure that all communications are strictly related to careers and alumni related activities. Any inappropriate or concerning communications should be reported to the Headteacher. The school reserves the right to investigate any reported professional misconduct on the platform.

3. Student Use of Digital Technology

3.1 Chromebooks for Learning:

- Chromebooks are permitted and encouraged in school for educational purposes.
- Students are responsible for the care and appropriate use of their assigned Chromebook. Where the device is obtained through the school's Chromebook partner, any damages or issues should be reported to the IT manager. All other devices may require an external provider for support.
- Students must use their school accounts for all school-related activities. This includes:
    - Saving files to their designated Google Drive folders.
    - Using approved applications and extensions.
    - Refraining from attempting to access or modify system settings.
    - Not using the account for personal non school related activities.
- Access to all websites and online services may be restricted by the school's filtering system.
- Students must not attempt to bypass security measures such as firewalls or content filters. Inappropriate content includes, but is not limited to, pornography, violent content,

hate speech, material promoting illegal activities, and content that could be considered bullying or harassment.
- Students must not share their login details with others.
- Students should report any issues, damages or concerns to their teacher and/or the IT Manager.

3.2 Personal Devices:

- The use of mobile phones and other personal devices is prohibited during school hours for lower school students, in all areas of the school. Phones should be switched off and stored in bags all day.
- Sixth Form students may be permitted to use devices within the Sixth Form block only.
- In some cases a personal device may be deemed necessary, for example for the use of medical monitoring equipment. In these cases the device should be only used when required and should not be used to make calls, send messages etc.
    - Audio and video recording are prohibited without explicit permission from all individuals involved. Head of School approval must be obtained. All data should be stored in compliance with the GDPR policy.
    - Students must respect the privacy of others and refrain from using personal devices in a manner that disrupts the learning environment.
- The school is not responsible for the loss or damage of any personal devices.

3.3 School devices:

- School devices are monitored using a range of technologies. Anything saved to or created on a school device is subject to review to ensure compliance with this policy. There should be no expectation of privacy when using school allocated accounts or hardware, even from home.
- School devices remain the property of The Cottesloe School. All issues relating to school devices should be reported to the IT Team.
- Any damage to school property will be investigated. Should malicious damage be discovered a charge for repair or replacement will be raised. Costs will be based on the replacement value of the device.

4. Acceptable Use Guidelines for All Users

All devices and connections within the school are monitored and managed by the IT Team. The school uses controls including firewalls, proxy servers and key logging, which can be used to review usage at any time.

4.1 Respectful Communication:

All online communication must be respectful and appropriate. This includes avoiding:

- Cyberbullying: Sending or posting harmful or mean content.

- Harassment: Repeatedly sending unwanted messages or making online contact.
- Discriminatory language: Using language that targets individuals or groups based on race, religion, gender, sexual orientation, disability, or other protected characteristics.
- Sharing private information about others without their consent.

4.2 Responsible use of AI:

- Students may use approved AI tools for educational purposes, as directed by their teachers.
- Students must properly cite any AI-generated content or ideas, adhering to academic integrity standards.
- Students are prohibited from using AI tools to generate content that is plagiarized, harmful, or violates school policies.
- Staff are to use AI tools in a way that aligns with data protection laws, and professional standards. Staff should also be aware of the potential for bias within AI generated content.
- The school reserves the right to monitor and regulate the use of AI tools on school devices and networks.
- Please refer to the The Cottesloe School AI policy for more details.

4.3 Privacy:

Users must respect the privacy of others and not share personal information without consent, in line with the school GDPR Policy.

When a room is provided with a digital display or projector, staff must ensure that sensitive data is not displayed by using appropriate settings to limit display to be visible to the teacher only

4.4 Copyright and Intellectual Property:

Users must respect copyright laws and intellectual property rights. Unauthorized copying or distribution of copyrighted material is prohibited.

4.5 Security:

Users must not attempt to access unauthorized systems or data, distribute malware, or engage in any activity that could compromise the security of the school's network or devices.

- All staff must ensure that screens are locked or logged out if not in use.
- Passwords and login information should not be shared or written down
- Any suspicious activity observed on school accounts should be reported to the IT team.

4.6 Data Protection:

All users must adhere to The Cottesloe School Data Protection Policy.

- Any suspected data breaches should be reported to the Data Protection Lead

5. Potential Breaches and Consequences

Any suspected incidents of digital system misuse or breach of this policy will be subject to investigation by the school.

School staff are permitted to confiscate any devices where misuse is suspected. Devices will be returned in accordance with the school mobile phone use policy and/or behaviour for learning policy.

Breaches of this policy may result in the following actions, depending on the severity of the infraction:

For Students:

- Investigation into any reported incidents, which could result in sanctions up to Fixed Term Exclusion (FTE).
- Reporting to any relevant agencies where the incident warrants it (for example the Police)
- Confiscation of device
- Loss of network/internet access
- Permanent Exclusion (in severe cases)

For Staff:

- Verbal warning
- Written warning
- Referral to line manager
- Disciplinary action, up to and including dismissal
- Referral to relevant authorities (in cases of illegal activity)

6. Review and Updates

This policy will be reviewed and updated annually to reflect changes in technology and best practices. All members of the school community will be notified of any significant changes.

7. Reporting Concerns

For Staff:

Any concerns regarding the misuse of digital technology by staff should be reported using a low-level concern form or directly to the Headteacher.

For Students:

Any concerns regarding the misuse of digital technology by students should be reported to a teacher, head of year or the lead or deputy designated safeguarding lead. Any related

behaviour incidents should be logged as per The Cottesloe School Behaviour for Learning policy.

8. Agreement

All staff and students (and their parents/guardians where applicable) will be required to acknowledge and agree to this policy upon joining the school.