THE MOUNTBATTEN SCHOOL

School Improvement Committee

Online Safety Policy

December 2025

Review Date: December 2027

Company No. 07560175

Whitenap Lane Romsey Hampshire SO51 5SY
t: 01794 502 502 e: info@mountbatten.school
w: www.mountbatten.school Company No. 07560175

Scope of the Policy

This policy applies to all members of the school community (including staff, students, governors, parents/carers, visitors, and community users) who access and use school ICT systems, both in and out of school.

The policy's scope extends to regulating student behaviour off-site and empowering staff to impose disciplinary penalties for inappropriate behaviour related to school membership, such as cyber-bullying or other online safety incidents. This includes the use of electronic devices and the deletion of data, consistent with the published Behaviour Policy and the 2011 Education Act.

Roles and Responsibilities

Trustees

Trustees are responsible for approving the Online Safety Policy and ensuring its effectiveness through oversight and monitoring. To fulfil this responsibility, Governors will:

• Receive annual reports from the Headteacher and Network Manager covering online safety incidents, filtering and monitoring summaries, and staff training updates.

• Review evidence of compliance with DfE Filtering and Monitoring Standards and KCSIE (Annex C) during the annual safeguarding audit.

• Ensure that online safety is a standing item within the Safeguarding or School Improvement Committee agenda.

• Verify that leadership and technical staff are taking effective steps to manage risks related to cybersecurity, safeguarding, and digital resilience.

Senior Leaders
The Senior Leadership Team maintains a duty of care for ensuring the online safety of the school community. Senior Leaders must be aware of procedures for serious online safety allegations against staff and ensure the Designated Safeguarding Lead receives suitable training.

Designated Safeguarding Leads
Designated Safeguarding Leads manage day-to-day online safety issues and liaise with technical staff, logging all incidents to inform future policy developments.

Network Manager and Team (Incorporating Technical Security Mandates)
The IT Services Team is responsible for ensuring the technical infrastructure is secure and protected from misuse or malicious attack. Specifically, the team must ensure:
• The school meets all required online safety technical requirements and guidance, including DfE "Filtering and Monitoring Standards" and KCSIE Annex C.
• The use of networks and devices is accessed through a properly enforced password protection policy.
• Filtering policy is applied, regularly updated, and its implementation is not the sole responsibility of a single person.
• The Network Manager oversees the patching schedule for all servers, devices, and applications.
• The use of the network, internet, and email is regularly monitored to report misuse to the School Business Manager and DSLs.
• Any significant technical incident is reported to the Director of School Services and the Data Protection Officer (DPO) when personal data is involved.
• Filtering and monitoring reports are reviewed termly by DSLs to ensure compliance and relevance.

Teaching and Support Staff (Incorporating Reporting Mandates)
Staff must ensure they are up-to-date on online safety matters and have signed the Staff Acceptable Use Policy (AUP). Staff must:
• Report any suspected misuse or problem to the School Business Manager, Director of School Services, Network Manager, or Pastoral Support.
• Report any suspected data breach immediately to the Data Protection Officer (DPO).
• Report any safeguarding concern to the Designated Safeguarding Lead (DSL).
• Ensure all digital communications with students/parents/carers are professional and conducted only using official school systems.

Technical Security, Authentication, and Data Management

The school is responsible for ensuring the infrastructure is safe and secure, implementing approved policies and procedures in line with NCSC technical standards and UKCIS guidance.

Authentication and Access Control (MFA and Password Standards)
• All users are provided with a username and secure password by IT Services, who maintain records.
• Users must adhere to minimum password standards: 12 characters minimum and must not contain personal information or dictionary words.
• Multi-Factor Authentication (MFA) is mandatory for all administrative, remote, and cloud-based accounts where possible.
• Staff password changes are required only when compromise is suspected (per NCSC guidance).
• The "administrator" passwords must be made available to the Headteacher or nominated senior leader if required.

Infrastructure and Monitoring
• School systems must meet recommended technical requirements and be protected by firewalls, endpoint protection, and intrusion prevention systems.
• Servers, wireless systems, and cabling must be securely located with restricted physical access.
• The IT Services Team must maintain vulnerability and patch management across all systems.
• Both on-premise and cloud platforms (Google Workspace, Microsoft 365) are monitored for suspicious activity and unauthorised access.
• All infrastructure, configuration, or security changes must be logged, reviewed, and authorised before implementation (Change Management).
• Filtering and monitoring must ensure students are protected from radicalisation, extremist, and illegal content, and changes must be authorised and logged.

Data Handling and Storage
Personal data must be recorded, processed, transferred, and made available according to UK GDPR and the Data Protection Act 2018.
• Personal data must only be stored on school-approved platforms (Google Workspace, Microsoft 365).
• Encryption is required for data at rest and in transit.
• Personal data transferred outside the secure network must be encrypted.
• When personal data is stored on portable systems or removable media, the data and device must be encrypted and password-protected.
• Use of removable media is restricted: Only encrypted USB devices approved by IT Services may be used.
• Any suspected data breach must be reported immediately to the DPO.

Mobile Technologies (Including BYOD/BYOT)

Mobile technology devices may be school-owned/provided or personally owned and may access the school's wireless network and cloud services.

• School-Owned Devices: All school-owned mobile devices must be enrolled in Mobile Device Management (MDM), allowing for encryption, remote wipe, and compliance enforcement.
• Personal Devices (BYOD): Any personal device used for school purposes must adhere to strict security controls:
  ◦ Must be encrypted and have automatic lock enabled.
  ◦ Must use PIN or biometric protection.
  ◦ Must access school systems only via secure apps or portals (preventing local storage of data).
• Staff are prohibited from connecting unauthorised network equipment (e.g., hotspots, routers, or VPNs) to the school network.

Staff Professional Communications and Use of New Technologies

Professional Communications
Digital communication between staff and students or parents/carers (email, social media, chat, VLE) must be professional in tone and content and may only take place on official (monitored) school systems. Staff must not use personal email addresses, text messaging, or personal social media for school-related communication.

Use of Artificial Intelligence (AI) and Cloud Tools
Staff must use AI-powered or cloud-based tools (e.g., ChatGPT, Copilot, Canva AI) only in line with the school's AI Policy.
• Staff are strictly prohibited from inputting or processing personal or sensitive information about staff, students, or parents in any AI system without prior authorisation.
• Any AI-generated content used for professional purposes must be fact-checked and appropriately attributed.

Social Media Conduct
Staff must maintain professional boundaries online. Personal social media must not reference or discuss the school, students, or colleagues. Where staff operate official school accounts, at least two authorised staff members must have access for oversight. Personal social media use during school hours must not interfere with professional duties.

Education and Training

Education & Training – Staff
All staff must receive online safety training and understand their responsibilities. Training is provided during annual safeguarding sessions and induction programmes.
• Training includes password security, phishing awareness, and the Acceptable Use Policy.
• The school may conduct phishing simulations to raise awareness.
• IT staff must complete annual technical security training (e.g., NCSC "Cyber Security for School Staff").

Education – Students
Online safety education is embedded throughout the Computing and Personal Development curriculum and revisited regularly through assemblies and tutorials. Students are taught to:
• Critically evaluate online content and misinformation.
• Recognise grooming, radicalisation, and coercive behaviours.
• Report harmful or illegal content.
• Protect personal information and digital footprint.

Education – Parents/Carers
The school will engage parents/carers through events such as Safer Internet Day, parents' evenings, and newsletters. Guidance will be provided on device filtering, parental controls, and online trends

affecting young people.

Unsuitable/Inappropriate Activities

The policy restricts the use of school systems and equipment for illegal or inappropriate purposes, including:

- Accessing or distributing illegal or harmful content (child abuse images, extremist material, racism).
- Bypassing school filtering/security controls.
- Engaging in online gambling, non-educational gaming, or private business use.
- Sharing confidential or proprietary information without authorisation.
- Creating or spreading malware.

Responding to Incidents of Misuse

In the event of suspected misuse, staff must follow procedures that involve:

- Having at least two senior staff members present during the investigation.
- Using a designated computer that can be isolated for evidence preservation.
- Logging URLs, time, and screenshots if appropriate (except where illegal material is involved).
- Immediately reporting illegal content (e.g., child abuse, grooming, extremist material) to the police.
- Isolating affected devices and preserving evidence without alteration.
- Reporting data-related incidents to the DPO and safeguarding issues to the DSL.

Policy Governance and Review

This policy operates alongside the Staff and Student Acceptable Use Policies (AUPs). Breaches of this policy or AUPs will be managed under the school's disciplinary framework.

This policy aligns with guidance from the UK Council for Internet Safety (UKCIS), the National Cyber Security Centre (NCSC), and Department for Education standards.

Signed by: …… Date: ……

Chair of Board of Trustees