

Packwood

Part of the Shrewsbury
School Family



Online Safety, Digital Technology, Social Media and Acceptable Use Policy

2026-2027

1. Purpose

Packwood School is committed to providing a safe, secure and supportive digital environment that promotes learning, protects pupils and staff from harm, and enables technology to be used responsibly and effectively. Online safety is recognised as a fundamental safeguarding responsibility and forms an integral part of the School's wider safeguarding and child protection framework.

This section of the policy establishes clear lines of accountability for online safety, cyber security, digital safeguarding, filtering and monitoring, acceptable use, social media engagement, and the use of emerging technologies, including artificial intelligence.

This policy applies whenever individuals access School-owned devices, networks, cloud services, communication systems, educational platforms or School information, whether on or off site.

2. Leadership, Accountability and Oversight

The Governing Body has strategic responsibility for ensuring that Packwood School maintains effective arrangements for online safety, cyber security, digital safeguarding, filtering and monitoring, and data protection. Governors will receive regular reports regarding online safety incidents, safeguarding concerns involving technology, emerging digital risks, cyber security matters and the effectiveness of the School's filtering and monitoring arrangements. The Governing Body will ensure that online safety remains a core element of the School's safeguarding culture and compliance framework. The Governing Body will appoint a governor with responsibility for safeguarding and online safety oversight who will receive appropriate reports regarding filtering, monitoring and digital safeguarding arrangements.

The Head has overall responsibility for the implementation, effectiveness and review of this policy. The Head is responsible for ensuring that appropriate resources, staffing, training, technical controls and safeguarding measures are in place to maintain a secure digital environment and to promote the safe, responsible and ethical use of technology throughout the School community.

The Deputy Head (Pastoral Care and Safeguarding) serves as the School's strategic lead for Online Safety and, where designated by the School, acts as the Designated Safeguarding Lead (DSL). The DSL has operational responsibility for the identification, assessment, recording and management of online safeguarding concerns. This includes concerns relating to cyberbullying, online exploitation, child-on-child abuse, harmful content, harmful contact, online grooming, sextortion, cybercrime, radicalisation, inappropriate use of artificial intelligence and any other safeguarding concerns arising through digital technology. Online concerns will be managed in accordance with Packwood School's Child Protection and Safeguarding Policy and relevant statutory guidance. The effectiveness of filtering and monitoring systems will be formally

reviewed at least once during each academic year with support from the Designated Safeguarding Lead, IT Services Team and relevant governors. A written record of these reviews, findings and actions taken will be maintained.

The Assistant Head (Boarding and Wellbeing) supports the safeguarding and wellbeing of pupils within the boarding community and works closely with the DSL to address risks associated with mobile technology, social media, online relationships, gaming platforms and out-of-school digital conduct.

Deputy Designated Safeguarding Leads support the DSL in fulfilling safeguarding responsibilities and ensure that safeguarding expertise remains available throughout the School day, during educational visits and whenever boarders are under the School's care. Current DSL and DDSL arrangements will be published within the School's Child Protection and Safeguarding Policy and communicated annually to staff, pupils and parents.

The Network Manager, IT Services Team and Digital Learning Leads are responsible for maintaining the security, resilience and effective operation of the School's digital infrastructure. They work collaboratively with safeguarding leaders to ensure that technical controls, monitoring arrangements and cyber security measures support pupil welfare and comply with current Department for Education expectations.

All members of staff are responsible for promoting positive digital citizenship, modelling safe and professional online behaviour, maintaining appropriate professional boundaries and reporting concerns promptly in accordance with safeguarding procedures.

3. School Digital Infrastructure and Technical Safeguards

Packwood School operates a secure and professionally managed digital environment designed to support education, communication, administration and safeguarding whilst protecting pupils, staff and School information.

The School utilises a range of enterprise-level systems and services, including:

- Microsoft 365 Education, including Outlook, Teams, OneDrive and associated productivity applications;
- Centrally managed user accounts and identity management systems;
- Secure cloud-based file storage and backup solutions;
- Managed wired and wireless network infrastructure across the School estate;
- Approved educational technology platforms and digital learning systems;
- Filtering and monitoring systems designed to meet current Department for Education filtering and monitoring standards;
- Endpoint management and device security systems;
- Threat detection and cyber security protection services;

- Multi-factor authentication and enhanced access controls where appropriate.

The School adopts a layered approach to cyber security and digital safeguarding through technical controls, staff training, user education, filtering, monitoring, secure authentication processes and effective safeguarding oversight.

Filtering systems are designed to protect users from illegal, harmful, extremist, inappropriate or age-inappropriate content. Monitoring systems are used to identify safeguarding concerns, inappropriate behaviour, cyber security risks and indicators of harm. The School recognises that no technical solution can eliminate risk entirely and therefore combines technical controls with education, supervision and safeguarding practice.

4. Monitoring and Use of School Systems

All School-owned devices, systems, networks, communication platforms and cloud services remain the property of Packwood School.

To fulfil its safeguarding, security, legal and operational responsibilities, the School reserves the right, where lawful, proportionate and necessary, to monitor, review, retrieve, preserve or disclose information created, stored, transmitted or received through School systems.

Monitoring may be undertaken for the purposes of:

- safeguarding pupils and staff;
- investigating safeguarding concerns;
- preventing cyber security threats;
- ensuring compliance with School policies;
- investigating allegations of misconduct;
- protecting School data and information assets;
- complying with legal and regulatory obligations.

Users should have a limited expectation of privacy when using School systems. Monitoring will only take place where lawful, proportionate, necessary and consistent with the School's safeguarding, legal and operational responsibilities.

Monitoring, access to information and data handling activities will be undertaken in accordance with UK GDPR, the Data Protection Act 2018, the School's Data Protection Policy, Privacy Notices and Records Retention Policy.

The School will maintain written records of filtering and monitoring reviews, system testing, safeguarding alerts, identified deficiencies and remedial actions. Records will be retained in accordance with the School's Records Retention Policy.

5. Artificial Intelligence and Emerging Technologies

Packwood School recognises the increasing role of artificial intelligence ("AI") and emerging digital technologies within education and acknowledges both the opportunities and risks these technologies present. The School recognises the safeguarding risks associated with digitally manipulated and AI-generated images, audio and video content, including the creation and distribution of synthetic or intimate imagery. Any such behaviour involving pupils will be treated as a safeguarding concern and managed in accordance with the Child Protection and Safeguarding Policy.

The School supports the responsible and educationally appropriate use of approved AI tools where they enhance teaching, learning, accessibility, productivity or administrative efficiency. However, AI must never replace professional judgement, safeguarding responsibilities or critical evaluation.

Any content generated through AI must be reviewed and verified by the user before it is relied upon, submitted, published or shared. Staff and pupils remain responsible for the accuracy, appropriateness and integrity of any work supported by AI technologies.

No member of the School community may enter personal data, safeguarding information, confidential School information, commercially sensitive information or special category data into publicly accessible AI systems unless expressly authorised and undertaken in accordance with School procedures.

Online safety forms part of the School's wider safeguarding risk assessment process. Emerging technologies, applications, online trends and safeguarding threats will be assessed regularly to ensure that policies, training and technical controls remain appropriate.

The use of artificial intelligence must comply with:

- UK GDPR;
- The Data Protection Act 2018;
- Copyright and intellectual property law;
- Academic integrity expectations;
- The School's safeguarding requirements;
- All relevant School policies and procedures.

The School will continue to monitor developments in artificial intelligence and emerging technologies and will update guidance, training and safeguards as risks, opportunities and regulatory requirements evolve.

6. Cyber Security and Reporting

All members of the School community have a responsibility to protect School systems and information from cyber threats. Suspected phishing emails, malware incidents, unauthorised access attempts, data breaches and other cyber

security concerns must be reported immediately to the IT Services Team and, where appropriate, the Designated Safeguarding Lead. Cyber security incidents will be managed in accordance with the School's incident response procedures.

7. Professional Conduct and Acceptable Use

All staff, governors, volunteers, contractors and authorised users are expected to act as positive role models and to demonstrate the highest standards of professionalism in their use of technology.

Users must:

- use School systems responsibly, lawfully and professionally;
- protect passwords and authentication credentials;
- safeguard confidential and personal information;
- respect copyright and intellectual property rights;
- maintain professional boundaries at all times;
- report safeguarding concerns, cyber security incidents and policy breaches promptly.
- Users must not:
 - access, create, store or distribute inappropriate, offensive or illegal content;
 - attempt to bypass security, filtering or monitoring systems;
 - misuse School data or confidential information;
 - access another user's account without authority;
 - communicate with pupils through unauthorised platforms;
 - engage in cyberbullying, harassment or conduct likely to bring the School into disrepute.

Failure to comply with this policy may result in disciplinary action, withdrawal of access rights, safeguarding intervention, referral to external agencies or legal action where appropriate.

Pupils and staff may only use personal devices in accordance with School procedures (see Annex A). The School reserves the right to investigate safeguarding concerns involving personal devices where such concerns affect members of the School community or impact pupil welfare.

8. Statement of Professional Responsibility

Packwood School expects all members of its community to uphold the highest standards of digital professionalism and online conduct.

Staff must not communicate privately with current pupils through personal social media accounts, personal email addresses, messaging services or other unauthorised platforms. All communication with pupils must occur through School-approved systems.

By reading this policy and accessing or using Packwood School's devices, systems, networks, platforms or digital services, all employees, governors, volunteers, contractors and authorised users acknowledge that they have read, understood and agree to comply with the requirements of this Policy, the Staff Code of Conduct and all associated Acceptable Use Agreements.

Individuals are expected to use technology safely, responsibly, professionally and lawfully at all times and in a manner that promotes the welfare of children, protects personal data, safeguards School information and upholds the reputation, values and standards of Packwood School.

Behaviour occurring outside school, including online activity taking place during evenings, weekends or holidays, may be investigated where it affects the welfare of pupils, members of the School community or the reputation of the School.