Penwortham Primary School

Acceptable User Agreement Framework Policy

2024-25

1. Introduction

1.1 Rationale

This Acceptable User Agreement Policy aims to provide clear guidance to all stakeholders on the responsible, ethical, and lawful use of the school's technological resources and infrastructure. It is designed to safeguard all users, particularly children, against the risks associated with online activity, while promoting digital literacy, monitoring compliance with statutory guidance, and supporting the school's broader safeguarding strategy.

This policy is informed by statutory requirements, including the Department for Education (DfE) guidance, such as Keeping Children Safe in Education (KCSIE, 2023), the Education Act 1996, and the Prevent Duty (2015). It supports the promotion of British values, fosters a safe online environment, and protects the school community from harm.

1.2 Audience and Scope

This policy applies to all users of the school's ICT systems and infrastructure, including staff, pupils, governors, volunteers, visitors, and contractors. It encompasses all technological devices owned or managed by the school (such as computers, laptops, tablets, and interactive whiteboards) as well as personal devices used for school activities, whether on-site or remotely.

Compliance with this policy is mandatory, and all users must familiarise themselves with its terms. Breaches will be addressed in accordance with the outlined consequences in this document.

2. Roles and Responsibilities

2.1 Governing Body

The Governing Body is responsible for ensuring the Acceptable User Agreement Policy reflects current statutory requirements and best practices. Governors must ensure that the policy is reviewed and updated annually, or sooner if legislation and guidance change.

2.2 Senior Leadership Team (SLT)

The SLT is responsible for implementing the policy across the school, promoting a culture of responsible technology use, and ensuring that all users understand and comply with it. The SLT must allocate resources for regular training on online safety and acceptable use for all staff and pupils, in accordance with the DfE's statutory guidance and the school's safeguarding policy.

2.3 Designated Safeguarding Lead (DSL)

The DSL is responsible for coordinating the school's approach to online safety, including responding to incidents or concerns where an online element is suspected or confirmed. The DSL works closely with the SLT to ensure that measures addressed in KCSIE are implemented effectively.

2.4 Teachers and Support Staff

Teachers and support staff are expected to model appropriate behaviour when using technology, enforce the policy within the classroom and school settings, and participate in ongoing training to remain informed about developments in online safety.

2.5 Parents/Carers

Parents and carers are integral to promoting the responsible and safe use of technology at home. They are encouraged to work with the school by reinforcing agreed expectations and monitoring their child's online activities to ensure compliance.

2.6 Pupils

Pupils are responsible for following this policy during their use of technology for school-related purposes. They must behave safely, respectfully, and responsibly, both while using school-owned equipment and during any educational activity that involves the use of digital tools.

3. Acceptable Uses of Technology

3.1 For Pupils

Pupils are expected to:

Use school devices, internet access, and software exclusively for educational purposes.

Treat school-owned technology with care and report any misuse or malfunctions to staff promptly.

Follow staff guidance when participating in virtual learning activities or using digital tools such as email services or collaborative platforms.

Demonstrate respectful behaviour towards others while communicating online, supporting anti-bullying efforts.

3.2 For Staff

Staff are expected to:

Ensure that all use of the school's ICT systems aligns with this policy and professional conduct expectations.

Use email, instant messaging, and other communication tools in a professional capacity only.

Protect sensitive pupil and school data, adhering to General Data Protection Regulation (GDPR) requirements.

Maintain professional boundaries on social media and refrain from connecting with pupils in private capacities.

3.3 For Visitors and Volunteers

Visitors and volunteers must use the school network and technology resources in accordance with their designated permissions and never violate safeguarding or data protection protocols. The use of personal devices on the school premises is restricted to circumstances approved by school leadership.

4. Unacceptable Uses of Technology

4.1 Prohibited Behaviours for All Users

Users must not:

Access, store, or share harmful, illegal, or explicit content.

Engage in online activities that involve bullying, harassment, or incitement of hatred.

Compromise the network by attempting unauthorised access or actions such as hacking.

Share login credentials or use another user's access rights.

Download or install unauthorised software or applications.

4.2 Consequences of Breach

Breaches of this policy will be taken seriously and may result in disciplinary action, including withdrawal of access privileges, involvement of external agencies, or formal sanctions in accordance with relevant legislation and safeguarding procedures as outlined in KCSIE.

5. E-Safety and Digital Literacy

5.1 School's Commitment to E-Safety

The school is committed to providing a secure and supportive online environment through regular e-safety education for pupils, staff, and parents. Pupils are taught about risks such as cyberbullying, phishing, and exposure to extremist material, and given the tools to navigate these challenges safely, in accordance with the Teaching Online Safety in Schools (2019) guidance.

5.2 Age-Appropriate Digital Literacy Education

Programmes tailored to each key stage are delivered using the UK Council for Internet Safety's Education for a Connected World Framework. Topics include recognising online risks, managing privacy, and engaging in positive digital behaviours.

6. Data Security and Privacy

6.1 Handling of Data

All users must comply with GDPR legislation when accessing, storing, or sharing data. Pupil records and sensitive information must only be processed through secure, approved systems, with multi-layer protection such as encryption and secure passwords in place.

6.2 Password Security

All users are responsible for creating strong passwords and changing them regularly. Passwords should never be shared, written down, or stored in an unsecure location.

7. Monitoring and Filtering

7.1 Network Management

The school utilises robust monitoring systems to track and filter all internet traffic on school-managed systems. This ensures compliance with both the KCSIE guidance and safeguarding duties.

7.2 Safe Internet Access

Filtering software is configured to block inappropriate websites, malicious applications, and harmful content, including material promoting extremism, self-harm, or hate speech.

8. Training and Communication

The school ensures mandatory e-safety training for all staff as part of their induction, with refresher sessions provided regularly. Pupils receive education on responsible technology use during PSHE and computing lessons. Parents receive guidance during e-safety workshops and through accessible resources shared on the school website.

9. Review and Evaluation

This policy is reviewed annually or when changes to statutory guidance necessitate an update. Feedback from key stakeholders, including staff and pupils, is incorporated to ensure its continued relevance and effectiveness.

10. Associated Policies

This policy operates in conjunction with:

Safeguarding and Child Protection Policy

Behaviour Policy

Anti-Bullying Policy

Data Protection Policy

11. User Agreements

11.1 Staff Acceptable User Agreement

Staff must sign a formal acknowledgment confirming their understanding of and agreement to comply with this policy, including explicit provisions about data security and the safeguarding of pupils.

11.2 Pupil Acceptable User Agreement

Simplified user agreements appropriate for different key stages will be provided, outlining expectations for the use of school ICT. These agreements may include visual aids or simplified language for younger users.

11.3 Parent/Carer Acceptable User Agreement

Parents and carers are invited to sign agreements confirming their understanding of the policy and their support for ensuring their child's compliance with it.

Conclusion

The school's Acceptable User Agreement Policy underpins a commitment to safe, responsible, and effective use of technology. Adherence to this framework ensures compliance with legal requirements, protects the entire school community, and supports pupils in becoming responsible and digitally literate citizens.

Agreed on date: ___________________________ Review
date:__________________________

By____(Headteacher)

By____(Governor)