Acceptable Use Agreement

Committee ownership for this policy: F&R, C&A, E&C, FGB	FGB
Must be approved by FGB: Y / N	
Required by: 1 / 2 • Where 1 is indicated, the requirement is statutory • Where 2 is indicated, the requirement is recommended	2
Frequency of review: annually, bi-annually, every 3 years	Annually
Date last reviewed:	September 2025
Date of next review:	September 2026
Display on website: Y / N	Y
Purpose:	To ensure that staff use technology safely and responsibly in line with KCSIE 2025. To protect children and staff from online harms and to safeguard the welfare of all.
Consultation:	Staff FGB
Links with other policies:	Keeping Children Safe Online Safety Staff Code of Conduct Data Protection

Should be signed by the Head Teacher and the Chair of Governors.

Signed by: Ardeep Virdi
Head Teacher
Date: _____

Signed by: Helen Oakley
Chair of Governors
Date: _____

This document outlines the Acceptable Use Agreement for all staff at Kew Riverside Primary School in line with statutory guidance from the Department for Education (DfE), including *Keeping Children Safe in Education* (KCSIE) 2025, the Teachers' Standards (DfE, 2011), and Ofsted's Education Inspection Framework (EIF, 2025).

This policy is part of the school's wider safeguarding and child protection framework and supports the ethos of promoting a safe and responsible digital environment for pupils and staff.

1. Purpose and Scope

1.1 Purpose of this Agreement

- To ensure that staff use technology safely and responsibly in line with KCSIE 2025.
- To protect children and staff from online harms and to safeguard the welfare of all.
- To support compliance with the Data Protection Act 2018 and the UK GDPR.

1.2 Scope

- Applies to all permanent, temporary, supply, and visiting staff.
- Covers use of school-owned and personal devices, including computers, laptops, tablets, mobile phones, and any other digital equipment.
- Applies both on the school premises and off-site when engaging in school-related activities or communications.

2. Legal and Regulatory Framework

2.1 Statutory Guidance and Legislation

- *Keeping Children Safe in Education* (KCSIE) 2025 – Staff must be aware of their duty to safeguard and promote the welfare of children (DfE).
- *Education Act 2002* – Duty to safeguard and promote the welfare of pupils.
- *Working Together to Safeguard Children* (DfE, 2018) – Multi-agency safeguarding responsibilities.
- *The Prevent Duty* (Section 26 of the Counter-Terrorism and Security Act 2015).
- *Data Protection Act 2018* and UK GDPR – To protect personal data and ensure safe handling of information.

2.2 Ofsted Inspection Framework

- *Education Inspection Framework* (EIF) 2025 – Inspectors will evaluate the effectiveness of safeguarding arrangements, including staff understanding of how to manage online safety risks, implementation of acceptable use policies, and the leadership culture in keeping children safe.

3. Professional Conduct

3.1 General Expectations

Staff must:

- Maintain professional behaviour at all times, both online and offline.
- Use school IT facilities and systems for professional or educational purposes only.
- Avoid conduct that may bring themselves, the school, or pupils into disrepute.
- Be role models for pupils in all aspects of digital responsibility.

3.2 Use of Personal Devices

Staff must:

- Not use personal devices for communication with pupils unless permission has been explicitly given by SLT and is in line with the school's safeguarding protocols.
- Ensure any personal devices used for work purposes are password-protected and in compliance with the school's Data Protection Policy.

3.3 Social Media Conduct

Staff must not:

- Communicate with current or former pupils via personal social media accounts.
- Post images of pupils without explicit written consent.
- Share confidential school information or derogatory comments about the school, pupils, parents, or colleagues.

Refer to the DfE's guidance: *Teaching Online Safety in Schools* (DfE, 2019), which sets out how to help children develop safe online behaviours by modelling appropriate adult behaviour.

4. Safeguarding and Child Protection

4.1 Reporting Concerns

- Staff have a duty to report any safeguarding or online safety concerns immediately to the Designated Safeguarding Lead (DSL) in line with the school's Safeguarding and Child Protection Policy.
- Incidents involving indecent or illegal material must be reported to the DSL and not investigated by the individual.

4.2 Online Risks

- Staff must be aware of risks such as cyberbullying, online radicalisation, sexting, and online grooming, as identified in KCSIE 2025 and referenced in Annex B.

- Regular training must be attended to stay informed of current trends and threats.

4.3 Use of Digital Images and Video

- Staff must ensure the safe and lawful use of digital media.
    - Written parental consent must be obtained before capturing or sharing images of children.
    - Images must only be stored on school-approved systems and deleted when no longer needed.

5. Data Protection and Privacy

5.1 Handling and Access to Data

- Only access personal data that is relevant and necessary for job functions.
- Do not store or transmit personal data via unencrypted or unauthorised methods.

5.2 Secure Use of Technology

Staff must:

- Use secure passwords and change them regularly.
- Always lock unattended screens.
- Log out of systems and devices after use.

6. Use of School IT Systems

6.1 Network Access and Monitoring

- Use of school systems is monitored in line with the school's monitoring and e-safety policies.
- Staff should have no expectation of privacy when using school IT systems.

6.2 Prohibited Use

Staff must not:

- Access, download or distribute any material that is illegal, offensive, obscene, or discriminatory.
- Use the school network or equipment for personal financial gain, gambling, political activity, or business purposes.

6.3 Email and Communication Systems

- School email accounts must be used for all professional correspondence.
- Communications with pupils must be conducted only through approved channels.

7. Training and Compliance

7.1 Mandatory Training

- Regular training on online safety, data protection, and safeguarding is required.
- Training includes guidance on current digital safeguarding risks and mitigative practice.

7.2 Staff Declaration

- All staff must confirm that they have read and understood this Acceptable Use Agreement as part of their induction and annually thereafter.
- Non-compliance may result in disciplinary action in line with the Staff Disciplinary Policy.

8. Review and Monitoring

8.1 Monitoring Compliance

- The school will regularly audit use of ICT systems and investigate any potential misuse.
- The DSL and SLT will monitor and review incidents and patterns to improve safeguarding.

8.2 Policy Review

- This policy will be reviewed annually or in response to changes in statutory guidance, notably updates to KCSIE.

Further Reading and References:

- Department for Education (2025) *Keeping Children Safe in Education*
- Department for Education (2019) *Teaching Online Safety in Schools*
- DfE (2018) *Working Together to Safeguard Children*
- Ofsted (2025) *Education Inspection Framework*
- National Cyber Security Centre (NCSC) *Protecting Devices and Data*
- United Kingdom General Data Protection Regulation (UK GDPR)
- Teachers' Standards (DfE, 2011)

This policy forms part of the school's safeguarding suite and should be read in conjunction with the Safeguarding and Child Protection Policy, the Online Safety Policy, the Code of Conduct, and the Data Protection Policy.