The Rivers
C. of E. Academy Trust

Acceptable Use Agreement

Cherry Orchard Primary School

Contents

1. Legal and Statutory Basis 2
2. Purpose 2
3. Responsibilities 3
4. General Principles 4
5. Filtering, Monitoring and AI Oversight 5
6. Internet Access 5
7. Unapproved Software 6
8. Bring Your Own Device (BYOD) 6
9. Data Security and Privacy 6
10. Unacceptable Use 7
11. User Credentials and Password security 8
12. Email 9
13. Internet 9
14. School devices and networks 9
15. Monitoring 10
16. Staff Training 10
17. Breach of Procedure and Reporting Misuse 10

1. Legal and Statutory Basis

This Acceptable Use Policy has been written in line with statutory guidance and sector standards, including:

- *Keeping Children Safe in Education* (KCSIE 2025)
- *Meeting digital and technology standards in schools and colleges* (DfE, 2023)
- *Cyber Security Standards for Schools and Colleges* (DfE, 2023)
- *Filtering and Monitoring Standards for Schools and Colleges* (DfE, 2023)
- Data Protection Act 2018 and UK GDPR
- Computer Misuse Act 1990
- Children and Families Act 2014
- Human Rights Act 1998
- Education Act 2002
- DfE guidance on *Generative AI: Product Safety Expectations* (2024)
  This policy should be read alongside the Trust's Safeguarding Policy, Data Protection Policy, and Online Safety Guidance**.**
- The Trust AI Policy

2. Purpose

This internal procedure defines how The Rivers C of E Multi Academy Trust ensures that users understand the acceptable and non-acceptable use of information technology assets, resources, and systems.

This procedure provides guidance that promotes proper, legal and responsible use of The Rivers C of E Multi Academy Trust's information technology assets.

In addition, this procedure supports the school in ensuring that its employees, students and contractors are aware of their responsibilities in using technology according to the following legislation:

- Communications Act
- Computer Misuse Act
- The Copyright (Computer Software) Amendment Act
- Copyright, Designs and Patents Act
- Criminal Justice and Public Order Act
- Data Protection Act, including the UK GDPR
- Defamation Act
- Electronic Communications Act
- Freedom of Information Act
- General Data Protection Regulation (EU GDPR)
- Human Rights Act
- Malicious Communication Act
- Regulation of Investigatory Powers Act

- Trade Marks Act

3. Responsibilities

All staff must use Trust systems, devices and online platforms responsibly, recognising the safeguarding risks associated with the *four Cs of online safety: content, contact, conduct and commerce*. Acceptable use applies to all digital activity carried out on Trust systems, whether onsite or remotely.

Headteacher

- Ensures staff are aware of and follow the Trust's acceptable use expectations, including use of personal devices and professional communication with pupils and colleagues.
- Embeds a culture of safe online practice and ensures breaches or concerns are acted on swiftly.
- Promotes understanding of the four Cs of online risk — harmful content (e.g. inappropriate or illegal material), unsafe contact (e.g. communication from unknown or predatory individuals), inappropriate conduct (e.g. cyberbullying or sharing personal data) and risky commerce (e.g. scams, commercial exploitation or gambling-style content).

Digital Lead

- Supports the Headteacher and DSL by providing strategic oversight of the school's digital systems and online safety practice.
- Monitors compliance with this policy, advises on emerging threats (e.g. AI, cyber security and disinformation) and helps coordinate staff training and monitoring activities in line with national guidance.
- The Digital Lead for Cherry Orchard Primary School is Caroline Jeynes.

Designated Safeguarding Lead (DSL)

- Provides leadership over online safety, including the *four Cs* and risks associated with AI misuse, misinformation and disinformation.
- Oversees the monitoring of staff online behaviour, acts on safeguarding alerts and ensures appropriate escalation to the Director of Inclusion or Education, Headteacher, HR or external agencies.
- Ensures staff receive regular training so they understand acceptable digital conduct and how filtering and monitoring protects pupils and staff.

Operations Manager

- Ensures this procedure is formally reviewed annually and updated in line with legislation and compliance frameworks, including *Keeping Children Safe in Education 2025*.
- Liaises with the IT Managed Support Service (Joskos) to ensure filtering and monitoring systems remain effective, are regularly tested, and reflect the school's risk profile.
- Ensures any required system changes are implemented promptly and that risks identified via filtering/monitoring are addressed.

IT Managed Support Service (Joskos)

- Works with CoConnect to implement, maintain and test the technical filtering and monitoring systems on behalf of the Trust.
- Alerts the Operations Manager, DSL and Headteacher to any failures or concerns arising from monitored activity.

- Ensures controls remain effective in preventing inappropriate access in relation to the *four Cs*.

☐ **All Staff**

- Must comply with this Acceptable Use Policy at all times and understand that any attempt to bypass controls, access blocked content without approval or use Trust systems inappropriately may result in disciplinary action.
- Must report any breaches or concerns immediately to the DSL or Headteacher, including incidents related to harmful content, inappropriate contact, unacceptable conduct or commercial exploitation online.

4. General Principles

4.1 Keeping passwords safe

All users with access to The Rivers C of E Multi Academy Trust's IT systems, services and devices must keep credentials, such as usernames, passwords and encryption keys secret in accordance with The Rivers C of E Multi Academy Trust's Password Procedure.

4.2 Locking devices when leaving unattended

All users accessing The Rivers C of E Multi Academy Trust's IT systems, services and devices must lock devices when leaving the room or breaking the line of sight.

4.3 Physically taking care of devices

All users with access to The Rivers C of E Multi Academy Trust's IT systems, services and devices must take all reasonable precautions to prevent loss, theft or damage to them.

4.4 Not using trust devices for inappropriate personal use

All users accessing The Rivers C of E Multi Academy Trust's IT systems, services and devices must do so without:

- Using inappropriate or offensive language, as defined within The Rivers C of E Multi Academy Trust's Staff Handbook.
- Bullying or intimidating others.
- Disclosing secrets or personal data in accordance with The Rivers C of E Multi Academy Trust's data protection procedure.
- Using them for personal entertainment or activities not related to school business without prior consent.

4.5 Not using trust devices to break the law

All users accessing The Rivers C of E Multi Academy Trust's IT systems, services and devices must take all reasonable precautions to prevent infringement of legislation identified within the purpose of this procedure.

4.6 Using IT in accordance with Safeguarding Procedure

All users accessing The Rivers C of E Multi Academy Trust's IT systems, services and devices must use them to support the trust's Safeguarding Procedure.

4.7 Using IT in accordance with Data Protection Procedure

All users accessing The Rivers C of E Multi Academy Trust's IT systems, services and devices must use them to support the trust's Data Protection Procedure.

4.8 Not avoiding technical controls designed to keep systems secure

All users accessing The Rivers C of E Multi Academy Trust's IT systems, services and devices must operate them according to how they were designed by the vendor. This includes, but is not limited to, the rooting or jailbreaking of devices.

4.9 Not using IT systems, services or devices that haven't been approved

All users accessing The Rivers C of E Multi Academy Trust's IT systems, services and devices must not use IT systems, services or devices that haven't been approved by The Rivers C of E Multi Academy Trust and their IT support service Joskos. We refer to this as shadow IT.

4.10 Using IT in accordance with our Cyber Security Incident Management Plan

All users accessing The Rivers C of E Multi Academy Trust's IT systems, services and devices must use them to support the trust's Cyber Security Incident Management Plan which includes reporting suspicious activity and confirmed incidents to Joskos.

4.11 Use of AI

AI must be used in accordance with the Trust AI Agreement.

5. Filtering, Monitoring and AI Oversight

The Trust uses centralised filtering and monitoring tools, managed by CoConnect, to prevent access to harmful, illegal or unsafe content. These controls are reviewed termly and audited annually to comply with DfE and KCSIE expectations.

All staff should report concerns about filtering or monitoring failures to the Designated Safeguarding Lead or the Headteacher.

Staff devices are included in filtering and monitoring.

The use of emerging technologies, including generative artificial intelligence (AI), will be monitored and restricted to educational contexts only. AI tools must not be used for personal content generation or to circumvent existing Trust policies on safeguarding, plagiarism or misrepresentation.

6. Internet Access

The Rivers C of E Multi Academy Trust provides internet access to all staff and students on its premises for usage relating to trust activities or teaching and learning.

Internet access is filtered to prevent use that does not support school activities or teaching and learning. This is done to reduce the risk of trust's devices becoming infected with malicious software (malware), in addition to supporting The Rivers C of E Multi Academy Trust's Safeguarding Procedure.

The Rivers C of E Multi Academy Trust expects all users to respect the web content filtering system, not purposefully circumvent it, and to report any inappropriate websites to Joskos.

Where additional credentials (such as passwords) are required specifically to access the internet (this includes connecting devices to the trust's wireless network for internet access) they must be kept secret and in accordance with The Rivers C of E Multi Academy Trust's Password Procedure.

Intentional inappropriate use may result in further restriction or removal of internet access. Severe or continuous inappropriate use may result in disciplinary action.

7. Unapproved Software

Unapproved software has not been checked for malware, authenticity, compatibility and compliance.

When new software (programs and web-based applications) is required, it should be requested through Joskos. Additionally, the trust's Data Protection Officer (DPO), Fyonna Lammas, should be contacted to ensure compliance with GDPR requirements.

8. Bring Your Own Device (BYOD)

BYOD is the use of personally owned devices for work purposes. This includes personal mobile phones and tablets for accessing any trust data, including emails and Microsoft Teams.

When connecting personally owned devices to The Rivers C of E Multi Academy Trust's wireless network, they must always be connected to the Rivers Guest Network which has been segregated from critical trust networks. Staff must remain vigilant when using the guest network, as most resources are hosted in the cloud.

Only devices that meet The Rivers C of E Multi Academy Trust's security requirements will be approved for BYOD.

BYOD devices must not be used for:

- Contacting students or their contacts for any reason other than in professional capacity
- Processing (this includes storing) images and videos of students or their contacts
- Processing (this includes storing) any other personal data relating to colleagues, students or their contacts
- Using software that hasn't been approved by the trust to process trust data.

If using a shared device at home to access trust data, a separate user account must be created; this should be password protected (this includes passcodes/face ID). Passwords must not be saved or shared.

We recognise that some staff may own and use smart watches that are linked to personal devices. These can be used under discretion of the headteacher.

If your personal mobile phones is used to access Trust resources, including emails and Microsoft Teams, if it is lost or stolen, it should be reported to both the Police and the school. We reserve the right to close staff accounts at any time.

9. Data Security and Privacy

Users of IT at The Rivers C of E Multi Academy Trust must always do so according to The Rivers C of E Multi Academy Trust's Data Protection Procedure.

Removable media (such as USB drives, SD Cards and CDs or DVDs) is not permitted, unless agreed by the Executive Team, and, where possible, has been prevented from being used with technical controls.

Users of IT at The Rivers C of E Multi Academy Trust are granted access to data only on a need to know basis according to The Rivers C of E Multi Academy Trust's Access Control Procedure. All user permissions are recorded in the Trust's permission register; if access to a system or resource is granted, it must be logged, reviewed regularly, and removed when no longer required.

Users of IT at The Rivers C of E Multi Academy Trust are responsible for facilitating security updates on The Rivers C of E Multi Academy Trust devices. This means regularly restarting devices, especially when prompted to do so by the device.

Users of IT at The Rivers C of E Multi Academy Trust have responsibility for the trust's Data Protection Officer (DPO) if they suspect a breach involving personal data.

The Rivers C of E Multi Academy Trust's support service, Joskos, ensures that the trust IT networks use an appropriate level of encryption. Users of IT at The Rivers C of E Multi Academy Trust have a responsibility for using the encryption tools made available to them to encrypt sensitive files leaving the trust's network by upload or email.

Social Media and Online Professionalism

- When representing the school online, neutral opinions must be expressed, confidential information must not be disclosed and information that may affect reputability may not be published.
- School devices must not be used to access personal social networking sites, unless it is beneficial to material being taught; permission must be gained from the headteacher before accessing the site.
- Pupils should not be communicated with over personal networking sites.
- Parents should not be communicated with over personal networking sites within a professional capacity.
- Will not accept networking requests from pupils or parents (in a professional capacity) over personal networking sites.
- Privacy settings should be applied to social networking sites.
- Defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, must not be posted on any online website.
- Contact with parents and carers must be carried out through authorised contact channels.

10. Unacceptable Use

The Rivers C of E Multi Academy Trust's information assets should not, under any circumstances be used for the acquisition, distribution, creation, processing, or storage of:

- Any form of material that can potentially be used to promote discrimination based on but not limited to disability, race, sexual orientation or gender.
- Any form of material that can be used to bully, victimise, or harass others.
- Unlawful material that violates intellectual property and privacy rights.
- Any form of material that directly or indirectly seeks to promote unlawful actions that may be threatening, extremist, or defamatory.
- Any form of material that may be regarded as obscene, indecent or offensive.

- Promoting, endorsing or distributing *misinformation, disinformation, conspiracy theories* or harmful content, including through AI-generated material.
- Using generative AI tools or services (e.g., ChatGPT, image generation, or similar) without prior approval and supervision from the headteacher or IT service lead.
- Engaging in commercial, gambling or influencer activities online using school systems.
- Using generative AI to create deepfakes, spoofed content, or representations of pupils, staff or parents.

11. User Credentials and Password security

All issued user credentials should be kept safe and secret in accordance with The Rivers C of E Multi Academy Trust's Password Procedure. It is unacceptable to display passwords or store them in a location that is easily accessible, for example, writing down passwords and sticking them onto a computer or desk.

Multi-factor authentication should be installed, by Joskos, on all staff devices. It should also be used where offered on any external websites.

All users are required to change passwords when there is suspicion that they may have been involved in a data breach, have been notified by haveibeenpwned or when requested by Joskos.

Unless explicitly authorised by Joskos, user accounts should never be shared. Users should not log into a computer system to access resources or services using another user's credentials.

Multi-Factor Authentication (MFA) must be enabled and used on all Trust systems and services that support it, including cloud-based platforms such as Microsoft 365. Joskos will install and configure MFA on Trust devices, and users must not disable or attempt to bypass it. Where external services or websites offer MFA, users are expected to activate it to protect sensitive information and prevent unauthorised access. This is a requirement under the DfE's Cyber Security Standards.

From 31 October 2025, any user who has not enabled MFA on their Microsoft account will no longer be able to access their Trust email or Microsoft 365 services.

12. Email

- All users should be aware of the risks associated with using email as described in the RPA approved cyber security awareness training and apply the techniques described in this training when handling emails.
- It is unacceptable to knowingly send or attempt to send an email with a malicious attachment or link with the intent of causing harm or disruption.
- As described in the RPA approved cyber security awareness training, all users should carefully check received emails for suspicious links or attachments before clicking or responding. All suspicious emails should be reported to Joskos or by using the self-report Microsoft button.

13. Internet

As explained in this procedure, the main purpose of The Rivers C of E Multi Academy Trust’s internet connection is to support teaching, learning, and administrative operations, and any activity that might disrupt this is unacceptable.

- Accessing the internet for personal use or non-work-related purposes is acceptable but limited.
- All users shall be responsible for the websites they visit and the activities they conduct on the internet.
- It is unacceptable to indulge in any personal or non-work activity that consumes significant network bandwidth such as downloading large files or live streaming.
- It is unacceptable to livestream classroom events.

14. School devices and networks

- It is unacceptable to attempt to bypass network security controls or filters.
- Where devices are shared, users should log out to prevent other users from using their credentials.
- Where the trust issues a device intended for remote working, only approved users should use such devices. If user-owned devices are permitted to externally access The Rivers C of E Multi Academy Trust's data or services, only approved users should use this access.
- It is unacceptable to download, store, copy, or distribute unlicensed material which may be subject to intellectual property and copyright laws.
- It is unacceptable to use tools that may degrade the network, scan ports, intercept network traffic, scan for vulnerabilities, reroute network traffic or alter the network configuration without approval.
- It is unacceptable to use devices in contravention of the Computer Misuse Act 1990, which makes the following an offence:
    - Unauthorised access to computer material. This refers to entering a computer system without permission (such as hacking).
    - Unauthorised access to computer materials with intent to commit a further crime. This refers to entering a computer system to steal data or destroy a device or network (such as planting a virus).

  - Unauthorised modification of data. This refers to modifying or deleting data and also covers the introduction of malware or spyware onto a computer (electronic vandalism and theft of information).
  - Making, supplying or obtaining anything which can be used in computer misuse offences.

15. Monitoring

The Rivers C of E Multi Academy Trust reserves the right to record and monitor the use of its IT network and facilities, subject to the Regulation of Investigatory Powers Act, for reasons including:

- Ensuring IT services and facilities remain effective and operational.
- The prevention, detection and investigation of a breach of the law, this procedure or other The Rivers C of E Multi Academy Trust policies, procedures or standards.
- Investigation of suspected misconduct by users including staff and students, such as plagiarism.
- Gathering information to respond to Data Subject Access Requests.
- Investigation of suspected cyber security incidents and data breaches.
- Conducting training exercises and preparing for information security incidents.

This includes, but is not limited to, monitoring and, where appropriate, recording of:

- Internet browsing data.
- Internet connection data.
- Communications, including email transactions and telephone calls.
- User device access and activity logs.
- User data access and activity logs.
- Bandwidth usage.
- Only authorised personnel from The Rivers C of E Multi Academy Trust's Joskos may record and monitor the use of its IT network and facilities.

Use of the internet is monitored by the trust central team.

16. Staff Training

All staff are required to complete annual cyber security awareness training, which includes specific modules on phishing, social engineering and secure data handling. Staff should also receive AI training as per current guidance.

17. Breach of Procedure and Reporting Misuse

Any form of violation towards this procedure may call for disciplinary measures under The Rivers C of E Multi Academy Trust's staff disciplinary policies.

Any misuse by pupils or staff members must be reported to the headteacher.