Staff Acceptable Use of Personal Devices Agreement

Rise Multi Academy Trust recognises that staff may wish to access Trust or school information using their own personal devices. While this can support flexible and effective working, it also introduces risks to information security that must be properly managed. The Trust always endeavour to provide all staff with their own Trust device and this agreement covers all staff using their own personal devices for work.

The Trust remains the *Data Controller* for all personal data accessed or processed on personal devices and is responsible for ensuring compliance with UK GDPR and the Data Protection Act 2018.

This Acceptable Use of Personal Devices document applies to:

- phones, tablets, laptops
- any personal device used for school systems

Use of personal devices for work purposes must be approved and registered with the Trust prior to access being granted.

1. Responsibilities of Staff

Any member of staff using a personal device to access Trust or school data must ensure that:

- The device is secured using encryption, not just password protection
- Strong authentication is in place (e.g. PIN, passcode, 2FA, biometric security)
- The device is configured to automatically lock after a short period of inactivity
- Appropriate security updates and antivirus protections (where applicable) are maintained
- Devices comply with Trust-defined security requirements, which may include Mobile Device Management (MDM), secure applications, or conditional access controls

The Trust will provide guidance and support to help staff ensure their devices meet these requirements.

Failure to implement appropriate security measures may result in disciplinary action if data is compromised or accessed unlawfully by a third party.

2. Data Protection and Security

Staff share responsibility with the Trust for protecting any Trust or school data accessed on their personal device and must follow all Trust policies and controls.

This includes ensuring that:

- Data is accessed, stored, and transmitted securely at all times
- Sensitive or confidential information is not shared inappropriately
- Devices are not used in a way that risks unauthorised access

Trust data should not be stored locally on personal devices unless strictly necessary, and approved cloud-based systems must be used wherever possible.

Personal devices must not be used to access or store highly sensitive data (such as safeguarding records) unless explicitly authorised.

When accessing data from home, public Wi-Fi, or while travelling, staff must use:

- Secure connections
- Approved cloud services only

Where required, staff must use Trust-approved secure access methods (such as VPN or conditional access controls).

Use of public or unsecured Wi-Fi must be avoided unless appropriate security protections are in place.

Any suspected or actual data breach must be reported immediately.

3. Monitoring and Access Control

The Trust reserves the right to:

- Monitor access to its systems
- Restrict or remove access from personal devices at any time
- Audit compliance with this policy

4. Images and Media

Pupil images or videos must not be stored on personal devices unless authorised. Where authorised:

- They must be transferred securely to Trust systems as soon as possible
- They must be deleted promptly from the personal device

Personal messaging or social media platforms (such as WhatsApp) must not be used to capture, store, or share school-related images or data.

5. Loss, Theft, or Compromise

In the event that a personal device used for work purposes is lost, stolen, or accessed by an unauthorised person, staff must report this as soon as reasonably practicable to the Headteacher or a member of the Senior Leadership Team.

This will be escalated to the Trust Infrastructure Lead and Trust Data Protection Lead.

Staff agree that the Trust may take appropriate action to protect data, including:

- Remote removal of Trust data
- Disabling access to systems
- Enforcing security controls

6. Disposal and Transfer of Devices

When a device is replaced, transferred, sold, gifted, or disposed of, staff must ensure that:

- All Trust or school-related data is securely deleted
- Any accounts or access permissions are removed
- Data cannot be recovered by any third party

7. Compliance with Trust Policies

All staff must read, understand, and comply with the Trust's Information Security Protocol and any related policies.

8. Data Rights and Complaints

Staff must support the Trust in meeting its legal obligations, including:

- Subject Access Requests (SARs)
- Data breach investigations
- Data protection complaints

This may include providing access to any personal device used for work purposes where relevant to an investigation or request.

Please refer to section 9 – Personal Device Usage Agreement and return to the school office or Rise Multi Academy Trust GDPR Lead, Nicky Hearfield at admin@risemat.co.uk once signed. Thank you.

9. Personal Device Usage Agreement

By signing this agreement, I confirm that:

- I understand my responsibilities when using a personal device to access Trust or school data
- I will ensure that my device is appropriately secured with encryption and access controls
- I will comply with Trust policies and share responsibility for protecting data
- I will report any loss, theft, or suspected breach immediately
- I will securely remove all Trust data when the device is no longer in use for work purposes
- I have read and understood the Trust Information Security Protocol
- I agree to the Trust applying security controls, monitoring access, and removing Trust data from my device where necessary to protect information

Name:

Signed:

Date:

Rise Acceptable Use of Personal Devices Agreement
Review cycle: Every two years (or following significant regulatory or operational change)