STAFF – ACCEPTABLE USE OF PERSONAL DEVICES

Ivy Education Trust recognises that many staff choose to access Trust information from their own devices.

Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption, that is above and beyond a simple password protection.

Staff must ensure that personal devices such as mobile smart phones, tablets and other portable electronic equipment are set to lock and only open with encrypted passcodes to prevent unauthorised access.

School will support and enable staff to ensure that their devices are compliant.

If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.

Encryption protection advice and guidance can be found at Appendix 1 to this document.

Own device usage agreement

I understand and accept that should I choose to access Trust data on any personal device that I use or own, this must have and use suitable encryption to secure the data.

Any unlawful access of data on such a device will be my responsibility. I will report any theft or loss to the DPO as soon as is practicable.

When exchanging, gifting, upgrading or selling the device I shall ensure that access to any school data is removed and data that relates to school is securely deleted.

Name:

Signed:

Dated:

Appendix 1

Quick Guide: Encryption on Personal Devices

This guide highlights **how encryption is typically enabled** on personal devices and **what staff must do** to remain compliant with the Staff – Acceptable Use of Personal Devices Policy.

How Encryption Is Typically Enabled

Mobile Phones & Tablets (iOS / Android)

- Modern smartphones and tablets use **built-in full-disk encryption**
- Encryption is normally enabled **automatically once a strong PIN or password is set**
- Biometric options (fingerprint / Face ID) may be used, but **only alongside a strong passcode**

Staff should ensure: - A strong PIN or password is set (not a simple 4-digit code) - Automatic screen locking is enabled - The device is kept up to date.

Laptops (Windows / macOS / Linux)

- Encryption often needs to be **enabled manually**
- Common built-in options include:
    - Windows: device or full-disk encryption
    - macOS: full-disk encryption
    - Linux: disk encryption during or after setup

Staff should ensure: - Full-disk or device encryption is switched on - A strong login password is used - The device locks automatically when not in use.

What Staff Must Do

1. **Check your personal device settings** to confirm encryption is enabled
2. **Use a strong password or passcode** at all times
3. Enable automatic locking when the device is unattended
4. Use biometrics only as an additional security feature, not instead of a password
5. Ensure work-related data is only accessed on encrypted devices

---

Getting Help

- Guidance for enabling encryption is widely available online for all device types
- Search for: *"Enable encryption on [your device model]"*
- If you are unsure, or need confirmation, **contact the IT team for support**

Reminder: Staff are personally responsible for ensuring any personal device used for work purposes is encrypted and secured in line with Trust policy.