Ankermoor Academy

Dosthill Academy

Glascote Academy

Violet Way Academy

Fierté Multi Academy Trust

Policy for the safe use of colleague's personal data

Introduction

Under the General Data Protection Regulation (GDPR), as a trust we should be doing everything in our power to prevent a breach of personal data.

This includes ensuring the security of personal data we allow staff members to access from their own devices, such as laptops or phones, to prevent the data from being lost, stolen or accidentally leaked.

There are no specific rules on how we must do this, but we can take practical measures as advised by the ICO.

If we need to give staff access to personal data via their own devices, such as laptops, phones or tablets, it's more secure to store that data remotely, where we have more control over how it can be accessed, than to allow it to be saved onto personal devices.

Staff Responsibility

Staff agree to a general code of conduct that recognises the need to protect confidential data that is stored on, or accessed using, a mobile device.
This code of conduct includes but is not limited to:

- Doing what is necessary to ensure the adequate physical security of the Device.
- Maintaining the software configuration of the device – both the operating system and the applications installed.
- Preventing the storage of sensitive company data in unapproved applications on the device.
- Ensuring the device's security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes.
- Reporting a lost or stolen device immediately.

Whenever practical, keep the data on a secure cloud service.
Should it be necessary for staff members to store personal data such as phone numbers then consent should be given prior to giving this data. This consent can be withdrawn at any time along with the right of erasure of given details.

Devices storing any such information need to be secure ie: password/pin protected.

Emails on personal devices

Staff are allowed trust email access on their personal devices however the device must adhere to a strong password policy.
If this is not in place, the email system may automatically reject installation of school emails on the device.

Security Policy Requirements

Staff are responsible for securing their device to prevent sensitive data from being lost or compromised and to prevent viruses from being spread. Removal of security controls is prohibited. Staff are forbidden from copying sensitive data from email, calendar and contact applications to other applications on the device or to an unregistered personally owned device.

Wi-Fi Access to school network

Staff who connect to the Fierté network with a personally owned device will be allowed access to the school systems and resources available via the Internet.

Loss, Theft or Compromise

If the device is lost or stolen, or if it is believed to have been compromised in some way, the incident must be reported immediately to members of Executive Learning Team, Head Teacher and DPO.

Enforcement

Any members of staff identified as violating this policy may be subject to disciplinary action, which may include but not limited to:

- Account suspension
- Revocation of device access to the trust network
- Data removal from the device
- Employee Termination

Monitoring and Review

This policy is reviewed and approved by staff, trustees and governors.

Reviewed by:	Mrs. L. Webster Data Protection Officer	**Date:** October 2018
Approved by:	Mrs. V. Blundell Trust Chair	**Date:** October 2018
Next review due by:		**Date:** October 2019