The Auriga Academy Trust

Off Site Working Procedure

Contents

1 Introduction

The Trust recognises that working off-site, or remote or mobile working, is required in many roles and situations in the Trust and in school, but this brings with it a number of potential risks, to data protection, confidentiality and privacy.

This procedure supports the Trust's Data Protection Policy and provides guidance on how to minimise risks associated with working off-site in line with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

2 Scope and Responsibilities

This procedure applies to the data protection and security aspects of all off-site working, or remote or mobile working, carried out by anyone working for the Trust or any of its constituent schools, including permanent and temporary staff, volunteers, and governors.

Off-site working includes (but is not limited to):

- Marking
- Lesson planning
- School trips and visits
- Meetings (e.g. child protection, TAF, TAC, SEN etc)
- Diaries, jotters, note books
- Laptops, tablets and other school devices (e.g. camera, iPad, phone)
- Accessing school portals / 'OneDrive' remotely

The health and safety aspects of off-site working are **not** covered by this procedure.

All staff are responsible for reading, understanding and complying with this procedure if they carry out off-site working. All leaders are responsible for supervising and supporting their team to read, understand and comply with this procedure if they carry out off-site working.

3 Reducing off-site data

When considering working off-site, take the following into account:

- Does all of the information need to be taken off-site? Only take what you need for the task in hand.
- If the data is already available electronically, do you need it in hard copy too?

4 Secure transporting of data

The Trust / school must ensure that devices permitted to be taken off-site have appropriate security. These devices must be backed up to the server as soon as possible. Any photographs must be downloaded from all devices as soon as possible and then erased.

Common sense measures to ensure off site security must be taken – for example:

- Devices and documents must be kept secure when off-site, not left unattended in public areas, not left in cars overnight, and special care must be taken when in public or travelling on public transport.
- Devices and documents must not be left in sight in vehicles, i.e. they must be stored in the boot rather than on the passenger seats. IT devices must not be left in vehicles overnight.
- All electronic data must be worked on through the Trust's / school's network.
- Hard copy documents must not be kept with devices such as laptops or phones, as these are more likely to be targeted by thieves.

5 Secure working off-site

When working off-site, take the following into account:

- Ensure your screen or documents cannot be viewed by any non-staff, including friends, family members, visitors or members of the public. Take special care if you are working in a public place.
- Ensure any phone calls cannot be overheard by any non-staff, including friends, family members or members of the public.
- Keep the amount of data/documents taken or accessed off-site to the minimum necessary to complete the task.
- Where required by the school / Trust, sign out and in sensitive documents. This includes, but is not limited to, safeguarding / child protection documents, and documents on trips and visits.

- Any documents removed from the school / Trust site are the responsibility of the employee removing them. Employees are therefore responsible for ensuring locked storage is available for personal data, where appropriate.
- Any documents that need to be securely disposed of must be brought back to the school / Trust for secure disposal, not put in domestic or public bins.
- Loss, theft or unauthorised access to school / Trust devices or documents must be recorded on GDPRiS as a data breach and reported to the Headteacher and / or COO as soon as possible.
- Sensitive or personal data must never be saved on unencrypted portable devices / storage.
- Never leave devices or documents unattended in a public place, or allow your screen to be read by others.
- Never discuss confidential matters in a public area where you may be overheard / recorded by others.
- Never entrust documents to unauthorised persons for safekeeping.
- The Data Protection Policy must be followed at all times.
- Employees having remote meetings in their home for work purposes are responsible for ensuring the suitability of their environment and enabling appropriate meeting security.
- The **IT Usage Policy** must be followed at all times.

6 Loaned Equipment

All loaned equipment remains the property of the Trust / school and must be returned upon request.

All equipment and materials loaned to you for off-site working are supplied to you solely for the purpose of carrying out work on behalf of the Trust / school. This includes access to educational resources.

Any faults with school-owned equipment or any security concerns must be reported in the usual manner.

Employees are responsible for returning any equipment to the Trust / school for the purposes of repair, maintenance and portable appliance (PAT) testing.

7 Personal Devices

Where school / Trust applications are accessed on personal devices, passwords must not be stored and the Trust's / school's **IT Usage Policy** must be followed.

Where devices are shared with other home users, the employee must log out of all school / Trust systems / portals / cloud services.

Employees must not download documents on to any device which is shared with family members.