# Off Site Working Procedure

## Fairfield Primary School

Version 3

| | |
|---|---|
| **Last Reviewed** | **November 2026** |
| **Reviewed By (Name)** | **Mr R Birtwhistle** |
| **Job Role** | **Headteacher** |
| **Next Review Date** | **November 2027** |
| **Version produced Spring 2025** | Amendments indicated in green text. |

This document will be reviewed annually and sooner when significant changes are made to the law.

Guidance from the Department for Education about school policies can be found here: https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts/statutory-policies-for-schools-and-academy-trusts

# Contents

1. Introduction ..... 3
2. Scope and Responsibilities ..... 3
3. Reducing off-site data ..... 3
4. Secure transporting of data ..... 4
5. Secure working off-site ..... 4
6. Loaned Equipment ..... 5
7. Personal Devices ..... 5


Copyright: Education Data Hub

# 1. Introduction

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

- This procedure supports our 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).

- This policy will be read in conjunction with the school HR advice and guidance. This policy has been the subject of formal negotiation and consultation between Derbyshire County Council and the recognised Trade Unions and Professional Associations. Agreement and adoption were only reached by Schools Joint consultative Committee where it is used in conjunction with the DCC LA Acceptable Use of IT Advice and Guidance.

# 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 school 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?


Copyright: Education Data Hub

## 4. Secure transporting of data

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

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

- Devices and documents will be kept secure when off-site, not left unattended in public areas, not left in cars overnight, and special care will be taken when in public or travelling on public transport.
- Devices and documents will not be left in sight in vehicles, i.e. they will be stored in the boot rather than on the passenger seats. IT devices will not be left in vehicles overnight.
- All electronic data will be worked on through the school's network.
- Hard copy documents will 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 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 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 will be brought back to the school for secure disposal, not put in domestic or public bins.
- Loss, theft or unauthorised access to school devices or documents will be reported to the Headteacher as soon as possible.
- Sensitive or personal data will 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 will be followed at all times.


Copyright: Education Data Hub

- 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 Security and Acceptable Use Policy will be followed at all times.

## 6. Loaned Equipment

All loaned equipment remains the property of the school and will 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 school. This includes access to educational resources.

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

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

## 7. Personal Devices

Where school applications, including Microsoft 365, Outlook and Teams, are accessed on personal devices, users must comply with the school's Bring Your Own Device (BYOD) Policy and all associated security requirements. Personal devices must be secured with a password, PIN or biometric authentication and must not be used to store sensitive school data locally unless expressly authorised. Users must not share or disclose passwords and must protect credentials in accordance with the IT Security and Acceptable Use Policy.

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

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


Copyright: Education Data Hub