# Off Site Working Policy

## GDPR LA POLICY

## Review: Annually

## Next Review Date: June 2022

| Role | Name |
|---|---|
| Headteacher | Caroline Rodgers |
| Chair of Governors | Linda Mosley |
| Designated Governor | Linda Mosley – GDPR Governor |
| Designated Senior Lead | Caroline Rodgers – Headteacher<br>Jayne Saxton – SBO |

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

# Contents

## *8.1 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 General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

## *8.2 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 (eg child protection, TAF, TAC, SEN etc)
- Diaries, jotters, note books
- Laptop and other school devices (eg camera, iPad, phone)
- Accessing school portals / 'OneDrive' remotely

The health and safety aspects of offsite working are *not* covered by this procedure.

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

## *8.3 Reducing offsite data*

When considering working offsite, take the following into account:

- Can you work on-site?
- 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?



 

## *8.4 Secure transporting of data*

Devices being taken offsite should have appropriate security such as passwords on laptops and other devices and encryption on memory sticks, these devices should be backed up to the server as soon as possible. Any photographs should be downloaded from all devices as soon as possible and then erased.

Devices and documents must be kept secure when offsite, not left unattended, not left in cars overnight, and special care should be taken when in public or travelling on public transport.

Devices and documents should not be left in sight in vehicles ie should be stored in the boot rather than on the passenger seats.

Data should never be sent to a personal email address, all electronic data must be worked on through the school's network.

Hard copy documents should not be kept with devices which are more likely to be targeted by thieves, to reduce the risk of theft.

## *8.5 Secure working offsite*

When working offsite, 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 offsite 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 should 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 must be reported to the Headteacher as soon as possible.
- Sensitive or personal data should never be saved on a laptop, 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 ICT Security and Acceptable Use Policy must be followed at all times.

## *8.6 Loaned Equipment*

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

Any faults with school owned equipment or any security concerns should 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.

## *8.7 Personal Devices*

School applications should not be installed on personal devices without prior consultation with Headteacher.

Where school applications are accessed on personal devices, passwords should not be stored and BYOD procedures should be followed.

Where using devices which are shared with other home users, the employee is responsible for ensuring they log out of all school systems / portals / cloud services.

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



 

| Date | Details of Changes | Name | Approval Date | New Version No | Website |
|---|---|---|---|---|---|
| 23.7.20 | New policy cover sheet added<br><br>Page numbers on contents list amended | ES<br><br>JS | | One | |
| 10.3.21 | Retitled from Procedure to Policy on Front Cover<br><br>Page 3 – Wording amended from procedure to policy in the last paragraph | ES<br><br>ES | | Two | |
| 13.5.21 | Sentence added to policy cover sheet - This document will be reviewed annually and sooner when significant changes are made to the law<br><br>New contents page added<br><br>Section 8.2 – wording added to first sentence – and security<br><br>Section 8.2 – Paragraph 3 – wording changed from policy to procedure<br><br>Section 8.4 – Paragraph 3 – wording changed from 'onsite in cars' to 'in sight in vehicles'<br><br>Section 8.5 – Bullet points removed:<br>• School applications should not be installed on domestic PCs without prior consultation with the IT Lead and DPO.<br>• Where school applications are accessed on domestic devices, the passwords should not be stored.<br><br>Section 8.5 – Bullet point 5 added<br><br>Section 8.5 – Bullet point 7 – wording changed from DPO to Headteacher<br><br>Section 8.5 – Bullet point 8 – wording changed from 'moveable storage or tablet' to 'portable devices/storage'.<br><br>Section 8.5 – Bullet point 13 added<br><br>Section 8.5 – Bullet point 14 – wording added 'Security and<br><br>Section 8.6 – New section added to policy<br><br>Section 8.7 – New section added to policy | JS | | Three | |
| 16.6.21 | Section 8.4 Paragraph 3 – word change from 'site' to 'sight' | ES | | Four | |
| | | | | | |
| | | | | | |



 