BRAMLEY VALE PRIMARY SCHOOL

Every Child Every Day

Off Site Working Procedure

Bramley Vale Primary School

Version (1)

Owner	Bramley Vale Primary School
Author	Education Data Hub
Issue Date	May 2022
Review Date	May 2024
Statutory Yes/No	No

Version	Date of governors Approval	Changes Required
1	May 2022	Scheduled review

Contents

8.1 Introduction 3
8.2 Scope and Responsibilities 3
8.3 Reducing offsite data 4
8.4 Secure transporting of data 4
8.5 Secure working offsite 4

8.1 Introduction

- We recognise that working offsite, 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 offsite 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 aspects of all offsite working, or remote or mobile working, carried out by anyone working for the school, including permanent and temporary staff, volunteers, and governors.

Offsite 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 procedure if they may carry out offsite working.

8.3 Reducing offsite data

When considering working offsite, take the following into account:

- Can you work onsite?
- Does all of the information need to be taken offsite? 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 onsite in cars, 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.
- School applications should not be installed on domestic PCs without prior consultation with the IT Lead and DPO.
- Where school applications are accessed on domestic devices, the passwords should not be stored.
- 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 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 DPO as soon as possible.
- Sensitive or personal data should never be saved on a laptop, unencrypted moveable storage or tablet.
- 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 ICT Acceptable Use Policy must be followed at all times.
- The Data Protection Policy must be followed at all times.