Carleton Rode and Forncett St Peter Primary Federation

Work out of School Policy

Formally adopted by the Governing Board/Trust of:	**Carleton Rode & Forncett St. Peter CEVA Primary Federation**
On:	**11th March 2022**
Chair of Governors:	**Sally Richards**
Review due:	**March 2023**

If you would like to discuss anything in this privacy notice, please contact:

Data Protection Officer: dpo@dataprotection.education

If you would like a copy of any documentation, please contact the school office:

Forncett - 01508 530506

office@forncett.norfolk.sch.uk

Carleton Rode – 01953 789384

office@carletonrode-primary.norfolk.sch.uk

Document Version

Version	Author	Date	Approved by	Effective from
1.0 template	DPE	01 Jan 2019		
2.0	DPE	16 March 2020	JE	16 March 2020

Contents

Introduction

This policy statement can be included in your existing Data Protection Policy or Staff Code of Conduct. Alternatively, it can be adopted as a standalone policy.

The underlying principles of this policy are:

- Individuals are responsible for the data they are authorised to handle outside of the organisation and reasonable steps should be taken to secure data taking into account its value, sensitivity and confidentiality.
- The organization (and its managers) are responsible for the preparation of appropriate services to enable work out of school and to train and support staff in its execution.

Work out of school definition and purpose

In this policy statement, home working is defined as a formal arrangement where the member of staff is permitted to take work home overnight, at weekends or over the school holidays to complete projects or ad hoc work. This policy provides direction on how to safeguard electronic and physical data, including personal and non-personal data.

It also covers the circumstances where data is taken out of school for work purposes, for example, to make home visits by attendance officers, or by SLT for external meetings.

It covers all information handled on behalf of the organisation including data that is:

- accessed
- collected
- used
- shared
- stored
- disclosed
- disposed of

Criteria for taking data off-site

Where data is taken off-site each member of staff should have approval from management, undertaken work at home training and an agreement covering:

- The type and volume of data that can be moved off-site. This must be limited to only that which is required to complete the processing activity
- The purpose for which it is being taken
- The methods for transporting data off-site (physical and electronic)

Staff working from home must first have agreement from the organisational management to take and store work at home.

- The amount of home working expected, with maximum time limits
- The type of work that can be completed at home
- A suitable environment for working at home must exist
- Any requirements for reporting on home working

Work taken off-site must not be worked on in a public location and public wifi should be avoided.

Prior to any agreement, the organisation should ensure that the data and processing out-of-school is documented and risk assessed by the Data Protection Officer.

Communications with students must only ever take place using approved organisation communication protocols (e.g. using organisational email, not personal email accounts; using approved systems such as Google Classroom or other virtual learning environments).

Organisational communication, email and acceptable use policies must be followed when conducting work, even on a personal device.

Transportation of data

The greatest risk of data loss is when it is being moved.

Where possible access files using a secure, access-controlled cloud environment and avoid physical transportation of documents and storage devices.

- Physical files (paper documents) must be kept secure and in possession of the user at all times. No files will be left unattended in a vehicle or other unsecured location during transit.
- Physical devices (laptops/portable storage) must meet the standards set in the IT Policy. At a minimum, any devices must be encrypted.
- We do not recommend using USB memory sticks (or other portable storage) unless in exceptional circumstances. Any use of portable storage must be approved by management and only when encryption is available on the device.

In all cases follow these steps:

1. Management should agree the scope of off-site working (see criteria for taking data off-site) and the methods of offline working
2. Where access to data is not through cloud storage, remote desktop or virtual private networks, save any data on to an encrypted device whilst on-premises.
3. Where any physical data is being moved, record its removal from the site and ensure a signature of the custodian is obtained.
4. Physical files (paper documents) must be kept secure and in possession of the user at all times. No files will be left unattended in a vehicle or other unsecured location during transit. Where possible, reduce the visibility of documents in transit and when being stored.
5. Physical devices (laptops/portable storage) must meet the standards set in the IT Policy. At a minimum, any devices must be encrypted.

6. When working at the remote site, ensure that access to data is safeguarded. Do not share access to documents with non-authorised personnel and do not share the use of any device with not-authorised personnel. Do not share any passwords. Minimise screens if others can view data. Lock or turn off devices when not in use.
7. Physical confidential files must be kept securely (e.g. store in a cupboard, drawer or briefcase)
8. When back on-premise, return all data and physical devices to their secure locations and the custodian should sign for the return.

Home office arrangements

Staff working at home must have a suitable location for working that provides a dedicated workspace and meets the organisation's Health and Safety policy with respect to the Health and Safety at Work Act. This includes:

- Reviewing the home work area and ensuring you have an adequate and comfortable place to sit and work;
- Taking regular breaks.

Any concerns should be brought to senior management's attention immediately.

Staff working at home will ensure the confidentiality and security of any information they are required to work within the home, in accordance with their existing contract of employment, the organisational IT Policy, Data Protection Policy and Staff Code of Conduct.

Such information will not be accessible to family or visitors of the home worker.

Working in public

Working on private, confidential and personal data in public areas should be avoided.

Working via public WIFI should only take place if you have a VPN.

Use of public computers is not allowed.

Using your own IT equipment

Follow the organisational IT policy for standards to be applied to any personal IT equipment used for accessing work data. Where possible, a home technology assessment should be provided by the organisation IT department

At a minimum, if using your own equipment it must meet minimum standards for anti-virus, malware and operating system updates and security patches.

Personal devices accessing organisational data should employ access control to prevent access by unauthorised users. Consider setting up a work-specific profile. Use multi-factor authentication and secure passwords.

Avoid downloading documents to your home IT equipment. Where possible, share information in the cloud, especially for staff resources. If you have no choice but to download a document

to work on, discuss with your school leadership team prior and once you have completed and uploaded the document, delete from your home device and empty the recycle bin as well.

If you must download documents to your own device, create an encrypted folder and remove this folder from any synchronisation with personal backup solutions.

Remember, documents can be synced with the cloud so ensure no documents have been stored in your personal cloud space or backup.

Accessing the school server via a VPN/Remote Desktop

If you are using your own equipment avoid downloading documents and storing on your home equipment. If you VPN allows, use remote-desktop to work on the organisational device remotely.

Cloud access to services (e.g.Google drive, Office 365, Cloud MIS, CPOMS etc)

You should avoid downloading to your own device and work on the document online.

Using portable storage

USB sticks/portable hard drives and other portable storage should be used for short-term transportation of data only and only in exceptional circumstances. All files should be stored on the organisation's network and only required files stored on the device and then returned onto the network at the earliest opportunity and files on the device deleted. Any use of portable storage must be approved by management and only when encryption is available on the device.

Any devices or equipment provided by the employer for home working should be returned when the home working arrangement ends.

Insurance and related matters

The employer will extend its employer, public liability and professional liability insurance to cover staff working from home and taking data off-site, ensuring coverage of assets and data during transportation as well as storage at home. The organisation will ensure that any organisational equipment has adequate insurance cover for the locations it is used and during transportation.

The homeworker will contact their own insurers and mortgage lender or landlord to inform them of his/her intention to work at home in case of any additional costs and restrictions.

Availability of data

Whilst data may not be physically held by the organisation, the organisation must be able to retrieve and make available any such data in response to subject access requests under the Data Protection Act 2018, or Freedom of Information requests under the Freedom of Information Act 2000

Data Breaches and Information Incidents

If a data breach or information incident contact school management and the Data Protection Officer immediately, following the organisation's Data Breach Procedure. This would include (but not Data Protection Education can be emailed at dpo@dataprotection.education, or a data breach can be logged on the Data Protection Education Knowledge Bank be limited to) unauthorised disclosure or loss of equipment.

Data Protection Education can be emailed at dpo@dataprotection.education, or a data breach can be logged on the Data Protection Education Knowledge Bank