Rooksdown Parish Council

Data and Cyber Security Policy

V1 March 2019

1 Purpose

This document specified the steps that must be taken by councillors, officers and employees to limit the risk and impact of a data or cyber security breach.

Failure to abide by the provisions of this policy will be considered as a breach of the Code of Conduct for Councillors and will be dealt with as such.

2 Scope of the council's data processing facilities

2.1 Council IT systems

Rooksdown Parish Council (RPC) owns the following IT systems:

- A laptop for use by the Clerk

There is no internal network or server, or remote access.

Email and office app facilities are provided using Microsoft Office 365, to which the clerk and a named councillor (currently Tim Botten) have administrative access.

At the current time the only officer or employee of the council is the clerk. IT support for the clerk's IT is provided on a voluntary basis by Cllr Paul Lovett.

2.2 Councillor IT systems

Councillors use Office 365 to access email and files, though these may be copied onto personal devices.

2.3 Physical media

The following items are stored on paper in the council office:

- Signed copies of minutes
- Allotment application forms (where not received by email)
- Financial and day to day management documents

Councillors may print council documents and emails for personal use.

HR records that are required to be kept on paper (eg signed employment contracts) are stored securely by the Chairman either of the Council or the HR Committee if it exists.

3 Policy for use of IT devices

The following applies to all devices used to store council files and/or emails, whether owned by RPC, councillors, officers or employees, unless otherwise stated:

3.1 Passwords

All devices shall be protected by:

- EITHER a password containing:
    - At least 8 characters, including at least 1 each of the following:

        - Uppercase letter
        - Lowercase letter
        - Digit
        - Special character (!”£$%^&*()_-+={[}]:@~;’#<>?/)
- OR a local PIN that is not easily guessable
- OR fingerprint, retina or face recognition.

3.2 Council-owned device storage

When not in use, such devices must be kept in either:

- In a locked building where there is no public access (eg the clerk’s home)
- Where there is public access, in a locked container (eg a filing cabinet) in a room locked when not in use.

3.3 Office 365 password

All Office 365 accounts must be protected by a password conforming to the rules specified in 3.1 above

3.4 Updates

All updates to operating systems, security software, and applications used for council work must be updated as soon as reasonably practical after they are made available by the manufacturer.

3.5 Security software

Firewalls must be used where available. For Windows 10 devices Defender must be used, and for all devices with Windows operating systems earlier than Windows 10, effective antivirus software must be installed and used.

3.6 Encryption

Unless permanently stored in a dwelling that is locked when not in use (eg a councillor’s or officer’s home), all devices used to store council files and/or emails must as a minimum have this data encrypted:

- Android devices:
    - Those running v4.4 or above are automatically encrypted
    - Those running below v4.4 must not be used for council data unless they are shown to be encrypted.
- Apple devices:
    - Encryption is standard in all versions
    - For Mac devices File Vault disk encryption must be turned on as detailed in the Appendix to this document.
- Windows devices
    - Devices running Windows XP or below must not be used for council data
    - Devices running versions of Windows with BitLocker available (eg Windows 8 or 10 Pro and Enterprise) must be encrypted using BitLocker
    - Devices running versions of Windows without BitLocker must use VeraCrypt or similar third-party package to encrypt ideally the whole device but as a minimum all council files and emails.

If in any doubt, councillors and officers must ask the clerk for advice.

3.7 Data held on Office 365

When a councillor ceases to be member of the council, their Office 365 account will be immediately suspended and then deleted when no further access to the data is required by the council, usually within 30 days.

When an officer ceases to be employed by the council, access to their Office 365 account will be removed. Access to the account will usually be given to their replacement or another officer.

3.8 Removing council data from devices

When a councillor ceases to be a member or an officer ceases to be employed, they must remove all council data from all their devices. Similarly, when a councillor or officer no longer uses a device for council business, all council data on that device must be removed.

Data removal must be by either:

- physical destruction of the data storage
- or wiping with a suitable utility (ask the clerk for recommendation of a suitable utility at the time the device is changed).

In addition, council data must be permanently deleted on any associated cloud storage (other than the council's Office 365 system).

If required by the council or the clerk, the councillor or office must sign a statement that all data has been removed.

4 HR documents

All current HR documents must be stored in a secure Office 365 folder to which only the Chairman and Vice-chairman have access. Any HR documents that must be maintained on paper must be stored securely by the Chairman (either of the Council or the HR Committee if it exists) as described in section 5 below.

5 Physical media

Any physical media concerning council business (eg paper documents printed by or in the possession of councillors or officers) other than public documents must be:

- When not stored in a dwelling that is locked when not in use (eg a councillor's or officer's home), kept in a locked container, eg a filing cabinet
- Shredded as soon as they have been used for the purpose for which they were produced.

Note that theft or loss of any IT device containing council files and/or emails, or any loss of physical media concerning council business must be reported as a Data Breach.

MARTIN WHITTAKER

Clerk to Rooksdown Parish Council

Rooksdown Community Centre
Park Prewett Road, Basingstoke RG24 9XA

07928 129122

Appendix

How to turn on FileVault disk encryption:

1. Click on the Apple menu and select System Preferences.
2. Select Privacy & Security.
3. Click on the FileVault tab, then click the lock in the bottom left corner of the window.
4. Enter your administrator name and password and click Unlock.
5. Click “Turn On FileVault”
6. Choose whether you want to link your iCloud account to FileVault to unlock the disk and reset your password or create a recovery key and click Continue.
7. Click Restart to reboot your Mac and begin the encryption process.