RODBOROUGH
PARISH COUNCIL

Councillor IT Policy

Councillor Declaration on Page 11 For:

Name: _____

Adopted at Full Council on: 18th March 2025

Minute Reference: FC2425.301

Policy Review Date: Annual Council Meeting 2026

This policy is supplemental to, and does not in any way override, the Parish Council Standing Orders, Financial Regulations, Communications Policy, or GDPR Policy.

1. Table of Contents

2. Introduction

Rodborough Parish Council recognises that not all councillors will have equal access to personal IT equipment. The Parish Council commits to equipping councillors with the IT equipment to enable them to fully carry out the requirements of the role of councillor.

This typically includes:

- To access and respond to emails
- To attend online meetings or training sessions
- To access the summons, agenda and papers for council meetings It is also the case that some councillors may wish to use their own devices. The requirements for this are set out under section 3 'Bring Your Own Device'.

Parish Councillors must comply with this policy where they use a Parish Council device, or a 'Bring Your Own Device', as applicable.

This policy must be read in conjunction with other relevant ICT policies including:

- The Council's GDPR Policy
- Councillors' personal responsibilities and liability as a Data Controller and Data Processor.

3. Provision of IT Equipment

3.1 Equipment

Rodborough Parish Council will provide the following equipment to councillors who request it in order to carry out the requirements of the role:

1 x Laptop Computer
(Based on Lenovo IdeaPad 1, 15" HD Screen, 4GB Ram, Windows 11)

1 x Screen Protector / Carry Case

1 x External Keyboard (optional)

1 x External Mouse (optional)

1 x Microsoft 365 software subscription

3.2 Request

Requests for IT equipment shall be made to the Clerk who shall have delegated authority to place the necessary orders in accordance with this policy.

3.3 Replacement

Replacement shall be on a 4-yearly basis. This may be amended/extended on recommendation from the Parish Council's IT provider.

3.4 Appropriate Usage

- Councillors should use council issued IT equipment for council business only.
- Councillors will be held liable for the costs of any damage or loss resulting from inappropriate use.
- Councillors will be required to hand over IT equipment on request to Parish Council officers, including for the purposes of any necessary IT updates or upgrades.
- Councillors will undertake to adhere to the security requirements set out in the 'Bring Your Own Device' section below.

3.5 Security

- Passwords must be at least six characters and a combination of upper- and lower-case letters with a number and a symbol.
- Passwords must be kept confidential and must not be shared with family members or third parties.
- Passwords must be changed if it is disclosed to another person or discovered.
- The device must be set to lock itself with a password or PIN if it's idle for five minutes.
- Home Wi-Fi networks must be encrypted. Caution must be exercised when using public Wi-Fi networks as public Wi-Fi networks may not be secure.
- Public data backup and transfer services (Dropbox, Google Drive) must not be used
- Data must only be stored on internal memory, never on a removable memory cards
- Councillors must hand over the device to Officers on request where there is a personal data breach, a virus, or similar threat to the security of data.
- Councillors must return the device within 48 hours of ceasing to be a Rodborough Parish Councillor.
- Care must be taken to avoid using approved devices in a manner which could pose a risk to confidentiality, whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using Wi-Fi facilities in public places (e.g. coffee shops or airports), or Some apps for smartphones and tablets may be capable of accessing sensitive information.
- Lost or stolen devices must be reported to Rodborough Parish Council within 24 hours.

4. Bring Your Own Device (BYOD)

4.1 BYOD Introduction

Rodborough Parish Council grants Councillors the use smartphones and tablets of their choosing for council business.

This policy is intended to protect the security and integrity of personal data controlled and processed by Rodborough Parish Council.

Rodborough Parish Council reserves the right to revoke this privilege if Councillors do not abide by the policies and procedures outlined below. Rodborough Parish Council Councillors must agree to the terms and conditions set forth in this Bring Your Own Device (BYOD) policy in order to be able to connect their devices to the Town Council network.

4.2 BYOD Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed.
- Tablets including iPad and Android are allowed.
- Laptops are allowed.
- Connectivity issues may be supported by external IT assistance, but this will be on a case by case. In the first instance the connectivity issue should be reported to the Clerk.
- The device manufacturer or their carrier should be contacted for operating system or hardware related issues.

4.3 BYOD Security

- In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the Parish Council network.
- Passwords must be at least six characters and a combination of upper- and lower-case letters with a number and a symbol.
- Passwords must be kept confidential and must not be shared with family members or third parties.
- Passwords must be changed if it is disclosed to another person or discovered.
- Devices must be encrypted.
- The device must lock itself with a password or PIN if it is idle for five minutes.
- Caution must be exercised when using public Wi-Fi networks as public Wi-Fi networks may not be secure.
- Public data backup and transfer services (Dropbox, Google Drive) must not be used. The Microsoft 365 subscription provided by the Parish Council includes these functions.
- Data must only be stored on internal memory, never on a removable memory cards.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- All data relating to Rodborough Parish Council will be erased at the end of a Councillor's term.
- All data relating to Rodborough Parish Council will be erased if there is a personal data breach.

- All data relating to Rodborough Parish Council will be erased if there is a virus or similar threat to the security of data.
- Care must be taken to avoid using approved devices in a manner which could pose a risk to confidentiality, whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using Wi-Fi facilities in public places (e.g. coffee shops or airports), or apps for smartphones and tablets may be capable of accessing sensitive information.

4.4 BYOD Risks, Liabilities, and Disclaimers

- Lost or stolen devices must be reported to Rodborough Parish Council within 24 hours.
- Councillors are responsible for notifying their mobile carrier immediately upon loss of a device.
- Councillors must adhere to the Rodborough Parish Council's BYOD policy as outlined above.
- Councillors are personally liable for all costs associated with their device.

5. Communication

This section is supplementary to the Rodborough Parish Council Communications Policy.

5.1 Email (Internal or External Use)

On commencement of your term as Councillor, you will be assigned a rodborough.gov.uk email address for conducting communications related to Council business, receiving meeting papers and meeting summons.

Internet email is not a secure medium of communication; it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If you are sending confidential information by email this should be sent using password protected attachments where possible.

Email should be treated as any other documentation. If you would normally retain a certain document in hard copy you should retain the email.

Do not forward email messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the email.

Your email inbox should be checked on a regular basis.

As with many other records, email may be subject to discovery in litigation, or a Freedom of Information request. See section six below). Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of the facilities is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

Councillors will be required to surrender their email account and all of its contents to the Parish Clerk at the end of their term of office or if they decide to leave the Council.

5.2 Social Media

Councillors using their own social media accounts must ensure that any comment made is clearly identified as their own and not representative of the Council.

Where Councillors are delegated to post on behalf of the Parish Council, all posts should adhere to the Communications Policy.

5.3 Internet

Posting information on the internet, whether on a newsgroup, via a chat services such as WhatsApp or via email is no different from publishing information in the newspaper. If a posting is alleged to be defamatory, libellous, or harassing, the person making the posting and the Council could face legal claims for monetary damages.

Using Council internet facilities for the purpose of trading or carrying out any business activity other than Council business is strictly prohibited.

For the avoidance of doubt the matters set out above include use of wireless facilities.

6. Council Information Held in Private Email Accounts

This section is supplementary to the Rodborough Parish Council GDPR Policy.

Use of private email accounts for Council business and data is prohibited in order for the Council and its members to comply with GDPR and Freedom of Information legislation.

6.1 Freedom of Information Act (FOIA)

The Freedom of Information Act 2000 (FOIA) gives rights of public access to information held by public authorities.

This guidance is intended to clarify the legal status under FOIA of information relating to the business of a public authority held in private email accounts in particular, but also other media formats.

This guidance does not deal with exemptions which might be applicable to information held in private email accounts, only whether it may be held for the purposes of FOIA.

Key Facts:

- FOIA applies to official information held in private email accounts (and other media formats) when held on behalf of the public authority.
- It may be necessary to request relevant individuals to search private email accounts in particular cases.
- Adherence to good records management practice can assist in managing risks associated with the use of private email accounts for public authority business purposes.

What the FOIA Says:

Section three sets out the two legal principles by which it is established whether information is held for the purposes of FOIA.

> 3. (2) For the purposes of this Act, information is held by a public authority if—
>
> (a) it is held by the authority, otherwise than on behalf of another person, or
>
> (b) it is held by another person on behalf of the authority.

Under section 3(2)(a) information will be held by the public authority for the purposes of FOIA if it is held to any extent for its own purposes. Only if information is held solely on behalf of another person will the public authority not hold it for the purposes of FOIA.

Section 3(2)(b) provides that in circumstances where information is held by another person on behalf of the public authority, the information is considered to be held by the authority for the purposes of FOIA. It is this sub-section that is of relevance to information held in personal email accounts.

The Information Commissioner's Approach

The Information Commissioner states:

> *Information held in non-work personal email accounts (e.g. Hotmail, Yahoo and Gmail) may be subject to FOIA if it relates to the official business of the public authority.*
>
> *All such information which is held by someone who has a direct, formal connection with the public authority is potentially subject to FOIA regardless of whether it is held in an official or private email account. If the information held in a private account amounts to public authority business it is very likely to be held on behalf of the public authority in accordance with section 3(2)(b).*
>
> *This can apply to any public authority. For example, a Councillor may hold information relating to local authority business in his/her private email account on behalf of the local authority. The Commissioner is aware that the issue has also arisen in a central government context in relation to the use of non-work systems. There is a need to have a clear demarcation between Councillor and departmental work. In the local government context, there is the same need to have a clear demarcation between Council business and work for individuals as their local representative.*

Official information held in private email accounts must therefore have a clear demarcation between Council business and work for individuals as their local representative.

Information in private email accounts that does not relate to the business of the public authority will not be subject to FOIA, but this does not mean it will not need to be reviewed to decide whether it is relevant to the request.

Situations where information legitimately requested under FOIA includes relevant information held on private email accounts will be rare. However, when a request for information is received, public authorities must consider all locations where relevant information may be held. This may include private email accounts.

The ICO recommends that, as a matter of good practice, public authorities establish procedures for dealing with such situations. These should outline the relevant factors to be considered in deciding whether it is necessary to ask someone to search their private email account for information which might fall within the scope of an FOI request the public authority has received. Relevant factors are likely to include:

- the focus of the request, indicated by the words used by the requester.
- the subject matter of the information which falls within the scope of the request.
- how the issues to which the request relates have been handled within the public authority.
- by whom and to whom was the information sent and in what capacity (e.g. public servant or Councillor); and
- whether a private communication channel was used because no official channel was available at the time.

Where a public authority has decided that a relevant individual's personal email account may include information which falls within the scope of the request and which is not held elsewhere on the public authority's own system, it will need to ask that individual to search their account for any relevant information.

6.2 General Data Protection Regulation (GDPR)

GDPR provides a legal requirement for the protection of personal information. As a principle, all personal data should be encrypted (whether sent by information systems or accessed on a mobile device).

The ICO provides guidance on the area of data transfers. This means ensuring that information is adequately protected from the point of transmission. This can be achieved using secure methods. This will need to include network protection through encryption (called Transport Layer Security), protecting the Domain Network Service (DNS), protecting the integrity of the actual email in transit and having governance in place to reject untrusted / spoofing emails.

Rejecting untrusted emails reduces the risk of an individual inadvertently clicking malicious links and activating malware. Care needs to be taken to balance this with an approach which reduces the quarantining of legitimate correspondence.

Secure information exchange, however, refers to more than just email. It is about risk management, information governance and network security. There are a number of factors to be considered when sharing information.

There are three levels of Government classification for the handling of information. This scheme operates within the framework of the Official Secrets Act (1911), the Freedom of Information Act (2000) and the Data Protection Act (1998). The classification divides data into three categories – OFFICIAL, SECRET and TOP SECRET.

For councils (and many other public sector organisations such as Health, Fire and Rescue, Community Policing as well as Charities) there is only one classification – OFFICIAL. The threat profile, information risks and attackers may differ, but the OFFICIAL level is consistent across those public sector bodies. Indeed, all personal information protected under the Data Protection Act, including health and care information, is classified at this level.

Within this, OFFICIAL-SENSITIVE is not a separate level but instead is a handling caveat for a small subset of information which is marked as OFFICIAL which requires special handling by staff. For example, a Council committee report with personally identifiable information on individuals could all be marked as OFFICIAL SENSITIVE. In each of these cases, the marking of 'sensitive' is about the handling of the data and the 'need to know', i.e. who is allowed to see it.

7. Declaration

This declaration should be signed by the Councillor upon joining the Council, and/or where IT equipment is accepted.

☐ I wish to use my own IT device for Council business

☐ I wish to request a device issued by the Parish Council

Model Number:

Serial Number:

Date of Issue:

I confirm that I have read, understood, and accept the conditions of the Rodborough Parish Council IT Policy.

Councillor Name: _____

Councillor Signature: _____ Date: _____

Witnessed By:

Officer Name: _____

Officer Signature: _____ Date: _____

8. Policy Review

This policy will be reviewed each year at the Annual Council Meeting.

The next scheduled review is May 2026.