

PERSONAL EMAIL AND DEVICE ADVICE SHEET

1. INTRODUCTION

There are a number of very important reasons why local councils should obtain an appropriate gov.uk domain name for their council. Obtaining a gov.uk domain for your council website and email accounts demonstrates the council's official local government status.

Members of the public are becoming increasingly cyber security-aware, so a gov.uk domain can help to build trust and credibility and visibly demonstrates authenticity. Most people will now reasonably expect a local council to have a gov.uk domain name.

In addition to using an official domain name for the Council's website, a gov.uk domain should also be used to support the Council's official email accounts for both Officers and Councillors.

2. EMAILS

Councils must ensure that in addition to having an official gov.uk domain name it is important to have a secure, centrally managed email system that is safe, secure and based in the United Kingdom to ensure that it is being managed by UK GDPR legislation and is not subject to the GDPR rules of other countries.

Regardless of which system the Council may choose to host its emails, there are a number of key benefits to using a commercial email system rather than just a free email account.

Most commercial email systems provide a centralised dashboard that gives the council the ability to add, edit and remove users as appropriate. The Council can immediately suspend user access in an emergency and perhaps most importantly, it offers centralised searching of all data contained within the system for effective compliance with Data Subject Access Requests and Freedom of Information Requests.

As there is one central system for all the registered accounts at the domain, regardless of what computer or Internet connection is being used to access it, emails are less likely to be identified as spam and therefore more likely to be delivered. A business-grade email system with its own spam filters built-in is more likely to be able to learn the kinds of email received and will reduce the risk of incoming emails being marked as spam or rejected entirely.

3. DEVICES

GDPR has been in effect for some time now. It can be a complex subject with a number of areas and potential ways in which councils can unwittingly fall short of compliance.

One area that could potentially be an issue is the use of councillors using their own devices when sending or receiving emails. Many larger councils have issued their members with dedicated devices that are intended purely for council business. This is best practice but does rely on both cost and affordability.

It is also important to understand what type of device is suitable. There is a choice between laptop and tablet as Councillors require a portable device to bring to meetings.

Though laptops might be more cumbersome they are more flexible as they are larger, come with a keypad and Councillors can have software provided to read and create documentation. Providing a wireless mouse can also help improve accessibility and functionality.

Tablets are smaller, less intrusive and easier to transport but they can be limiting in their functionality and have a smaller screen size, which may cause some issues to those with poorer eyesight and less dexterity.

4. DEVICE ADVICE

The advice normally provided to most parish/town councils is that councillors are requested to remove any council email addresses from their personal devices.

Council members can access their email via webmail from any browser. It is a simple case of navigating to their parish/town council website. The web address should be available from the relevant officer or provider.

Councillors can easily bookmark the relevant page to enable speedier access.

There are many advantages of using webmail. These include:

- The removal of the danger of a security breach on a councillor's own device as the emails viewed on webmail are not downloaded to the device used to access them;
- Councillors should no longer experience access issues which are common when trying to access email from a device using an email client;
- Most devices will be able to retain password and log on information to enable easy access to the emails.

5. ORGANISATIONAL MEASURES

The council should have the following policies which all councillors should be aware of and be trained on regularly:

- Privacy Policy: This will state what type of personal data the council holds, how it stores it, how it processes it and with whom it shares the data with;
- Document retention and disposal policy: This will detail how long types of documents will be held for
- Data Breach policy: This will detail what staff and councillors should do if the security of data is compromised, ranging from incidents of theft and lost devices to data sent to a wrong email recipient

- Personal device acceptable use policy: This will detail how the device should be used for council matters, including the prohibition on saving documents to the device, the provision that the device automatically locks if inactive for a period of time and that a device must be password protected.

6. TECHNICAL MEASURES

These can range from the complex and costly to the simple, from measures that will need to be implemented by the council's IT provider to those that the Clerk can do. They may include the following:

- Registering the personal devices with a remote locate and wipe facility to maintain confidentiality of the data in the event of device loss or theft;
- Password protecting all devices, including ensuring that all councillor owned devices are password protected, to stop unauthorised access of the device;
- Setting, editing and printing restrictions on a document containing personal data;
- Password protecting or encrypting documents sent by email.

7. SCENARIOS

The following examples outline some of the scenarios that could face a Council:

A councillor has been provided with a dedicated council email address. Unfortunately, they fail to be re-elected and subsequently have to leave the council. If that councillor has configured their own personal device to send and receive email from a dedicated email address on the same domain as their council, then chances are those emails will be inadvertently stored on the personal device even after their departure from office.

From a security viewpoint, this device now contains public data that could potentially be read by anyone with access to the device. This poses a potential data breach issue and there is little the Council can do to enforce deletion and ensure that it has been carried out.

The above scenario is also relevant in the case of retirement, relocation to another area or stepping down for other personal reasons.

A councillor uses another email that is not their official parish/town council email. Their email may, for example, be an official email account that they have been provided by another Council, possibly a principal authority, or it could just be a basic email account provided by one of the many email hosting companies.

As part of their parish/town council responsibilities the councillor receives staffing information, which may include salary scales, medical information and other sensitive information.

The first issue is that the data is being controlled by the principal authority and the parish/town council has no authority over that email and cannot delete or do anything

else with it. The emails are subject to the principal authority's Data Protection Policy and processes and the responsibility of its Data Protection Officer.

If it is a generic email there is even less comeback and the emails may even be hosted abroad and subject to different GDPR requirements.

If the councillor leaves the parish/town council then the principal authority council now has the responsibility for another authority's emails and data, some of which may be sensitive.

It causes even greater issues in the case of a Freedom of Information request as the individual councillor may be required to provide access to that email address.

8. FURTHER INFORMATION

Councillors and officers can obtain further information from the following resources:

[Parish Councils Resource Pack \(ico.org.uk\)](https://ico.org.uk)

[Fact sheet for councils: the use of personal email addresses and devices \(ico.org.uk\)](https://ico.org.uk)

[The importance of secure email systems and GOV.UK domains for local councils - News \(nalc.gov.uk\)](https://nalc.gov.uk)