

COPYTHORNE PARISH COUNCIL MEETING – TUESDAY MARCH 14TH 2023

Item 11 – To receive and approve a report on the use by Councillors of Parish Council e-mail addresses.

Background

At the June 11th 2019 Council meeting (item 9, Minute 266/19) agreement was given for:-

“The Clerk to arrange for TLC to support the introduction of the tablets by their setting up of seven individual e-mail accounts for the members of the council.”

Between May and July 2020 the Samsung tablets were issued with guidance on how to use them. Each was separately issued to individual councillors with a Parish Council e-mail accounts set up on them with the following naming convention (firstname.surname@copythorne.org.uk)

Current Position

Although the Computer Misuse Policy that all councillors signed when receiving their tablet included the clause below, the use of the “council e-mail addresses” has been sporadic with some councillors not using them at all. Some of the tablets have been returned to the Clerk and are not currently in use.

11.3 You will be provided with an official Council electronic mail address which must be used at all times for Council business. You are requested to monitor and manage your electronic mail and calendar on a regular basis.

NALC; HALC; and the Information Commissioners Office all strongly advise that personal devices and personal e-mail addresses should not be used for Council business and that Council supplied e-mail addresses should be used.

The reasons for this (many relating to Data Protection and Security of Data) are set out in the attachments to this report which have come from the bodies named above.

Recommendation

That with effect from the end of May 2023, in accordance with guidance from NALC, HALC and the ICO all councillors are to use “Council e-mail addresses” and not personal e-mail addresses.

(To support this all tablets will be returned to the Clerk and re-configure for the Councillors taking office after the May 2023 Parish Council Elections. Training/guidance will be provided on how to use the e-mail addresses and the Samsung tablets themselves).

David Rigby

Clerk to Copythorne Parish Council

February 20th 2023



Hampshire ALC Key Topic Note – Use of Personal Email Addresses

Hampshire ALC strongly recommend councillors and employees use an email address provided to them by their council when carrying out council business. This not only protects the council, but it also protects the member and or employee as an individual. Using a dedicated council provided email address ensures any data contained within it remains the property of the council.

Importantly the council need to consider their obligations under the [Data Protection Act 2018](#). In terms of UK General Data Protection Regulations (GDPR), the council is seen as the data controller, and therefore the council has obligations relating to the confidentiality, integrity, and availability of **all** personal data it holds. This means that the council is accountable for any business the council conducts involving personal data on any device or through an email account. The [Information Commissioner's Office](#) (ICO) have produced a useful guide to the [General Data Protection Regulations](#).

The use of personal devices or email addresses raises the risk that personal data is processed for a different purpose to that originally intended when the data was collected. Inevitably, councillors and employees will collect personal data during their term of office or employment. Everyone has a responsibility to ensure they only use personal data for the purposes for which the council obtained it.

If copies of data are stored on several devices and/or email accounts there is an increased risk that it will become out of date or inaccurate over time, or that it is retained for longer than necessary. It would also be difficult for the council to control where the data ends up, thereby increasing the risk of a data breach.

In the event of a personal data breach, the council must be able to demonstrate that they've secured, controlled, or deleted all personal data on a particular device, which is difficult to do if council members are using email accounts that are either not provided by the council, or in addition to their council provided email account.

The council should also be aware that under the [Freedom of Information Act 2000](#), the council are obliged to formally respond to any request for information the council holds. This information includes information held in personal email accounts that are being used for council business. By using a council provided email address to conduct council business, the council can more easily access information held to meet their obligations under the legislation. Should the ICO receive a complaint regarding information provided by the council, any investigation would then also be limited to official council email addresses without the need to interrogate personal email accounts.

It is also worth considering that when a councillor resigns from their seat, or fails to be re-elected, the council can ensure that all data within that member's email account can either be deleted or forwarded within the council to another member or employee, and the account

closed down, ensuring any data within remains with the council and any risk of a potential data breach minimised.

Essential Resources

[Guide to Data Protection](#) (ICO website)

[Bring your own device – what should we consider?](#) (ICO website)

[Apply for your gov.uk domain name](#) (Gov.uk website)

This document reflects our advice based on our understanding of the current legislation and guidance and our knowledge of the sector. It is not however intended to be formal legal advice.

For more complex issues we are able to obtain initial specialist advice on legal, employment, financial and planning matters as part of your membership fee. Please contact us to access this service.

Fact sheet for councils: the use of personal email addresses and devices

This factsheet has been produced following a series of workshops and discussions with local councils across the UK and will be of interest to parish council clerks looking for steps they can take to improve their council's data protection compliance.

The majority of parish clerks attending the Society of Local Council Clerks (SLCC) Leadership in Action Conference 2019 ranked the use of personal email addresses and devices for council business as their top data protection concern.

The UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) don't say which email systems or devices should be used. But if the use of personal email addresses and devices is something your council does, you should be aware of the risks and the council's data protection obligations and responsibilities.



Fact: Councils must ensure the confidentiality, integrity and availability of all personal data they hold, even if the data is being processed through personal email accounts or is stored on a privately-owned device.

As a data controller, a council has obligations relating to the confidentiality, integrity and availability of all personal data it holds. This means that the council is accountable for any council business conducted involving personal data on any device or through any email account.

The use of personal devices and email accounts could raise the risk that personal data is processed for different purposes from which it was originally collected. All members of the council should ensure they know their responsibilities in terms of only using personal data for the purposes which the council obtained it.

If copies of data (such as email attachments) are stored on many different devices, there's an increased risk that it'll become out-of-date or inaccurate over time. There's also an increased risk that it'll be retained for longer than necessary, because it's difficult to keep track of copies.

You may also find it difficult to respond on time to a subject access request if you have to search multiple devices or if you aren't aware of all the devices on which personal data may be stored.

Questions to ask:

- What types of devices are in use?
- Who else uses the personal email account or privately-owned device, and who else has access?
- How can you control the data on the personal email account or privately-owned device (eg accuracy and retention)?
- How much consideration has been given to the data on the device being overlooked?



Fact: Councils must process personal data securely – which may be more difficult to achieve if it's being processed through personal email accounts or is stored on privately-owned devices.

Councils must have 'appropriate technical and organisational measures' in place to prevent the personal data it holds being accidentally or deliberately compromised. This includes physical and organisational security measures and also cybersecurity. If data is shared around multiple devices this introduces more points of failure and vulnerability.

There's no 'one size fits all' solution to information security. The UK GDPR doesn't define the security measures that you should have in place. It requires you to have a level of security that is 'appropriate' to the risks presented by your processing. What's appropriate for your council will depend on your own circumstances, the information you're processing, and the risks it presents.

As the data controller, the council must ensure that all processing of personal data under its control remains compliant, regardless of the ownership of the device used

to carry out the processing. If there's a personal data breach, you must be able to demonstrate that you've secured, controlled or deleted all personal data on a particular device.

Questions to ask:

- How secure are the devices (eg is the device password-protected and what is the risk of malware)?
- What if the device is lost or stolen – can you remotely locate it and wipe the data?
- What operating system is the privately-owned device running?
- How is data transferred to other devices, and how secure are these systems and/or devices?
- Is your council using or considering cloud storage?



Fact: Councils must demonstrate that they are UK GDPR-compliant, and the use of personal email accounts and privately-owned devices may make this more complicated.

The principle of accountability requires you to be able to demonstrate that you are complying with the UK GDPR, and have appropriate policies and processes in place. If personal devices or email accounts are being used, you should have an effective organisational policy in place to ensure that the associated risks are managed.

You'll also need to take steps to make sure your members are aware of the policy and that it is implemented. This could include training, monitoring and audits.

Questions to ask:

- If you're using personal email addresses and/or devices to process data for council business, do you have an acceptable use policy in place to manage this?
- Have you implemented appropriate security measures as outlined above?
- Have you documented the associated risks and subsequent decisions?
- Does your council need to review/update its current approach?

More information

For more information about the accountability principle with the UK GDPR, visit ico.org.uk and search '[accountability principle](#)'.

The challenges of using a personal email system or device are set out in more detail in the ICO's [Bring your own device \(BYOD\)](#) guidance – visit ico.org.uk and search 'BYOD'.

Joint Panel on Accountability and Governance – Practitioners’ Guide – March 2022 (a NALC Publication - www.nalc.gov.uk/jpag)

Extract from pages 55-56

The importance of secure email systems and GOV.UK

5.204. All authorities except Parish meetings must now have an official website. To comply with GDPR, councils should provide official email accounts for their councillors as well as for their Clerk and other officers.

5.205. When choosing a domain name for the council's website and emails, many local council websites are appropriately making use of the official GOV.UK domain (for example, ourparishcouncil.gov.uk), with email addresses being linked to that domain.

5.206. Using a GOV.UK domain for your council website and email accounts demonstrates the council's official local government status. Members of the public are increasingly cyber security aware, so a GOV.UK domain can also help to build trust, credibility⁵⁶ and visibly demonstrates authenticity. Many people will now reasonably expect a local council to have a GOV.UK domain name.

5.207. For the purposes of user management, councils should ensure that the Proper Officer can add and remove member and staff email accounts. Commercial ‘dashboard’ email and web systems offer centralised searching of all data contained within the system for effective compliance with GDPR Subject Access Requests and Freedom of Information Requests.