

## Notice of a meeting of the

### **Personnel and Administration Committee**

18<sup>th</sup> February 2020 at 7.30pm  
Park Room, Civic Hall, Didcot



#### **Admission of the public and media**

The council welcomes members of the public to its meetings in accordance with the Public Bodies (Admission to Meeting) Act 1960.

#### **Reports and minutes**

We add reports and minutes to our website.

#### **Recording, photographs and filming**

The press or public may audio-record, photograph or film meetings, or report from the meeting using social media. As such members of the public may be recorded or photographed during the meeting.

We ask that anyone wishing to record or photograph the meeting notifies the Town Clerk before the start of the meeting.

#### **Public participation**

The council welcomes the public's involvement in meetings, which must be in accordance with our rules (Standing Order 18-20 on a matter before the Committee).

At the relevant time during the meeting, the Chairman will invite members of the public to present their questions, statements or petitions.

To find out about participation contact the Town Clerk.

# Agenda

1. To receive apologies
2. To receive declarations of interest  
Members should declare any interests they may have on any item on this agenda in accordance with Didcot Town Council's Code of conduct.
3. To agree the minutes of the meeting held on 3<sup>rd</sup> February 2020 as a true record  
**(minutes attached)**
4. Questions on the minutes as to the progress of any item
5. To consider the need for Councillor mail boxes – *see report*

## EXCLUSION OF THE PRESS AND PUBLIC

Pursuant to Section 1 of the Public Bodies [Admission to Meetings] Act 1960 the committee will be asked to exclude the press and public from the meeting on the grounds that publicity would be prejudicial to the public interest by reason of the confidential nature of the business to be transacted

6. To review the Town Clerk's probation period – *six month review to be brought to the meeting.*



**Janet Wheeler**  
**Town Clerk**  
**12<sup>th</sup> February 2020**

**Voting Committee members:**

**Cllr M Khan (Chair); Cllr A Macdonald (Vice Chair); Cllr A Thompson; Cllr V Haval; Cllr E Hards**

**Nominated substitute Committee members:**

**Cllr M Walsh; Cllr P Giesberg; Cllr J Durman; Cllr A Sandiford**

## Didcot Town Council

---

### **Personnel and Administration Committee** Monday 03 February 2020 at 7.30pm Park Room, Didcot Civic Hall



## **Minutes**

Note: These minutes are subject to approval as a true and correct record by the next meeting of this committee.

### **Present:**

Cllr M Khan  
Cllr A Macdonald  
Cllr V Haval  
Cllr E Hards

### **Officers:**

Mrs J Wheeler (Town Clerk)

### **Public participation**

None

### **29. To receive apologies**

Apologies were received from Cllr A Thompson. Cllr J Durman was unavailable as a substitute.

### **30. Declarations of interest**

None

### **31. To approve the minutes of the last meeting held on 11<sup>th</sup> November 2019**

It was proposed by Cllr A Macdonald and seconded by Cllr V Haval to RESOLVED to approve the Minutes as a true record. Cllr E Hards amended minute 24 by deleting the words: "who is currently on the list of substitutes".

### **32. Questions on the Minutes**

There were no questions on the minutes.

### **33. To review the following documents from Oxfordshire Pension Fund:**

**The Administration Strategy** is the strategy taken by the Oxfordshire Pension Fund to manage the pensions of the council employees. They are currently consulting on some possible changes that may help them address the issues experienced during the processing of employee pensions. The measures proposed are:

- A charge of £150 for submission of incorrect data.
- A charge of £75 per return and/or £50 per employee to re-do the work due to incorrect information being supplied.
- A reduction in the time period for reminders from the current 10 days to 5 days

It was noted that pensions are becoming more complicated and the Finance Manager and the Town Clerk are not pensions experts.

It was proposed by Cllr Haval; seconded by Cllr A Macdonald to respond to bullet three of the consultation to request that the full ten days is allowed for reminders. The reasoning for this is that if staff have annual leave or are unable to respond so quickly due to work load – more time is needed to gather the information. The accuracy of the data is more likely to be correct if adequate time is allowed for response.

**The Fund's Data Retention Policy** – this policy is for noting as part of the Oxfordshire Pension Fund's way of dealing with sensitive personal data.

Adoption of the "**Participating Employer Personal Data** – The Town Clerk had reviewed the Town Council's current data retention policy and it did not really cover pension information. The Oxfordshire Pension Fund have reviewed their policy and it may be safer to adopt their template policy to ensure that the two dovetail together.

There was a discussion on whether a maximum of fifteen years retention for an employee was long enough. On the proposal of Cllr M Khan; seconded by Cllr A Macdonald it was AGREED to adopt the template in principle but query the recommended amount of time that we should keep individual's data and bring this back to the Personnel Committee.

### **34. To review the Town Clerk's probation period**

The Town Clerk went through the agreed targets at the three monthly review and then left the room for the next part of the meeting. The meeting then asked the Town Clerk to prepare for a further meeting of the Personnel and Administration Committee on 18<sup>th</sup> February 2020. In that time, Cllr M Khan would circulate an opportunity for Councillors; staff and some hall hirers to comment on the Town Clerk's performance. The feed back would be reviewed and a recommendation would be made to the next meeting of the Council on 2<sup>nd</sup> March 2020.

### **35. Exclusion of the press and public**

Proposed by Councillor A Macdonald, seconded by Councillor V Haval, it was:

**RESOLVED** to exclude the press and public from the meeting pursuant to Section 1 of the Public Bodies [Admission to Meetings] Act 1960 on the grounds that publicity

would be prejudicial to the public interest by reason of the confidential nature of the business to be transacted

**36. To review the salary increments for DTC staff for 2020 – 2021 financial year**

The list of staff who were due to be up by one spinal column point was noted in the Staffing Report.

It was proposed by Cllr E Hards; seconded by Cllr V Haval and RESOLVED to agree in principal and be forwarded to the next meeting of the Finance and General Purposes Committee on 24<sup>th</sup> February 2020.

**37. Staffing Report**

The Committee members considered a confidential staff report and two recommendations. The recommendation concerning the essential car users allowance was not agreed.

The recommendation regarding an accumulation of Time Off in Lieu (TOIL) was referred to the next meeting of the Finance & General Purposes Committee on 24<sup>th</sup> February 2020.

Finally congratulations were extended by a member of the Civic Hall Team who is expecting a baby in the summer.

The meeting closed at 9.30pm

Signed \_\_\_\_\_ Chair Date \_\_\_\_\_

## **Personnel and Administration Committee**

### **18<sup>th</sup> February 2020**

Report author: Janet Wheeler



## **Consideration of Councillor email-boxes**

### **Introduction**

1. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) state that the Council must ensure the confidentiality, integrity and availability of all personal data – even if the data is being processed through personal email accounts or is stored on a privately-owned device.

### **Detailed issues**

2. The ICO fact sheet (attached) for councils covers the risk and obligations as a data controller. The bottom line is that the council is accountable for any council business conducted involving personal data on any device or through any email account.
3. 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.
4. If copies of data such as email attachments are stored on different devices there is an increased risk that the information will become out of date or inaccurate over time.
5. It is also difficult to respond to subject access requests if you have to search multiple devices – or if you aren't aware of all the devices on which personal data may be stored.
6. The council is required to demonstrate that they are complying with GDPR and have appropriate policies and processes in place. If personal devices or email accounts are being used – the Town Council need to have an effective organisational policy in place to ensure that the associated risk is managed.

### **For consideration**

- A solution is to have dedicated Didcot Town Council mail boxes which are only used for Town Council business. Quite a few councils at our level have done this and more are complying when – like us – they are changing their IT system.

Advantages include:

- It standardises the emails by making it clear in which capacity the emails are being sent – especially useful for double or triple hatters!
- Control of the emails lies with the council and can be cut off when a councillor leaves.
- Easier to administrate FOI and subject access requests – this can be managed through the IT company to ensure complete impartiality.
- DTC's contractor could be asked to supply technical support for set up on iPad; laptops and desk tops for individual Councillors who need this help.
- Full admin rights can be held with the contractor to keep staff impartial.
- Limits can be set on data levels to control the amount of data stored. Individual controls can be put in place so that the Mayor or Committee Chairs have a greater storage capacity.
- It is possible to control outgoing messages to prevent forwarding or printing – or limit the amount of time the message can remain offline.
- It may be possible to include links to the website to reduce the amount of paper reports.
- Extra layers of security and encryption can be easily added.
- The cost is around £3.00 per mailbox a month (£63 per month) or £756 per annum.

Disadvantages include:

- Less freedom to archive information indefinitely.
- Extra cost.
- Another complication for Councillors who are less technically-minded.

### **Recommendation**

1. The advent of Councillor mailboxes has not been budgeted for so I would recommend that if the Committee wish to recommend this service – that it goes to the meeting of the Finance and General Purposes Committee on 24<sup>th</sup> February 2020.
2. Consider asking all Didcot Town Councillors to register as Data Controllers. This means that any data kept on councillor email or private email accounts is the responsibility of the individual Councillor. This is a cost that could be paid by the Town Council.

### **Risk and Legal Implications**

7. The risk of breach of data could carry a financial penalty and place the Town Council into disrepute.
8. Didcot Town Council needs to put in place measures to control the risk – especially to information going outside of the Council.

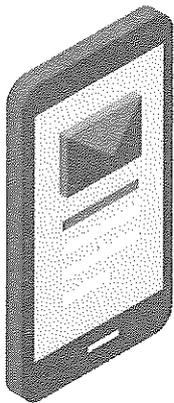
Janet Wheeler  
Town Clerk

# 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 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.

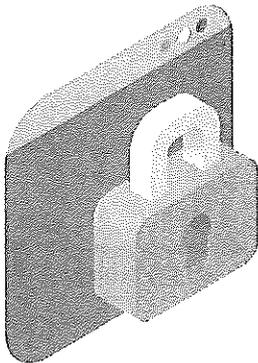
The use of personal devices and email accounts could raise the risk that personal data is processed for different purposes from which it was originally collected. All members of the council should ensure they know their responsibilities in terms of only using personal data for the purposes which the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

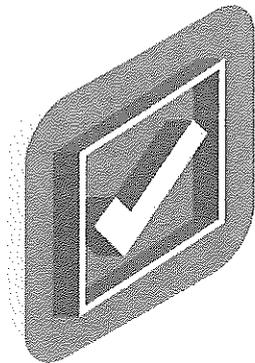
There's no 'one size fits all' solution to information security. The GDPR doesn't define the security measures that you should have in place. It requires you to have a level of security that is 'appropriate' to the risks presented by your processing. What's appropriate for your council will depend on 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 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 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 GDPR, visit [ico.org.uk](http://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](http://ico.org.uk) and search 'BYOD'.