Bearsted Parish Council

Data Handling Policy

Introduction

This is the Data Handling Policy for Bearsted Parish Council.
We have an obligation to handle data sensitively and securely, be that personally identifiable information or intellectual property. This policy describes our approach to data handling. Note that laws such as the General Data Protection Regulation (2018) and the revised Data Protection Act (2018) are also relevant, and where there is a conflict between them and this policy the law prevails.

Scope

This policy applies to, but is not limited to, all staff and contractors of the Council.

Your responsibilities

All persons covered by this policy have an obligation to protect our data to the best of their abilities, in conformance with this policy. You should make yourself familiar with this policy and relevant laws such as GDPR (2018) and the Data Protection Act (2018), and how they apply to you. Additionally, you should undertake whatever data protection training we provide you. You may be required to revise this training from time to time. Depending on your contract, the terms of this policy may persist after you leave the organisation – please speak to the Clerk if you have any queries.

What is data?

Data can be held electronically (e.g. online or saved to a computer) or physically (e.g. on paper). Data in both formats should be protected and handled appropriately. Data relates to any information generated by or handled by the organisation, and may include, but is not limited to:

- Employee records (HR, payroll)
- Client information
- Electoral role information
- Contractor and Consultant information
- Residents' information, including messages and emails.

Risks to data

A loss of data carries a significant risk to the organisation. Where the data is Personally Identifiable Information, there could be a significant impact to the individuals in question. We do not wish to cause harm to our employees, clients, or third parties. Loss of such data may also incur financial penalties to the Council.
In the event the lost data relates to our Intellectual Property, there could be a financial impact to the Council. This may result in the loss of income, directly affecting the Parish Council's ability to serve the community and potentially lead to the loss of jobs.

Storing data

Digital data (e.g. Word documents, emails, information in third party systems) should be stored only on devices and systems provided by us. Wherever possible, data should be stored in a shared folder, so it is (appropriately) accessible by other members of the Council. The easiest way to do this is to upload the files to SharePoint.

While you may store a local copy of the data, for example on your laptop, this must **not** be the only copy. Having a single copy of our data only on your device is prohibited, as in the event of your device failing or being stolen the data would be lost.

Paper documents should be stored appropriately, with access restricted to others on a need-to-know basis. Documents should be locked away when not in use to prevent loss or theft.

Our data must remain on approved software/systems. Access is permitted on personal devices but must be secured appropriately and access restricted.

When data is no longer required it must be securely deleted or disposed of. Data should be kept no longer than necessary.

Protecting data

Data should be "encrypted at rest" meaning that while it is not in use it cannot be accessed by a third party. For Council laptops this means the laptop will be encrypted with Microsoft BitLocker. Recovery keys for encrypted storage must be held by us to ensure encrypted data does not become inaccessible.

It is necessary to ensure data does not become inaccessible through loss or corruption. Data should be backed up, with backups stored separately from the original. The level of protection for the backup (e.g. encryption) must not be less than for the original copy. Backups will be kept according to our retention schedule.

Accessing data

You are provided with a user account to access your account/emails, and this account is unique to you. You should not share your password with anyone, nor should you allow someone else to use your account or devices while signed in to your account.

If a third party requires access to assist in troubleshooting or providing support, they are permitted to use your account **under your direct supervision**.

Monitoring data usage

You should be aware that we reserve the right to monitor usage of data, including, but not limited to, access, copying, transferring, and use of removable media.

Removable media

There are significant risks associated with removable media so usage should be avoided wherever possible. Removable media includes, but is not limited to:

- USB memory sticks ("dongles")
- Compact Disks (CD)
- Digital Versatile Disks (DVD)
- Media cards (e.g. SD cards, Compact flash cards)
- Mobile phones
- External hard disks
- Floppy disks
- Audio tapes
- Paper documents

Removable media is easily lost and stolen, resulting in the loss of data. Use of removable media also allows the easy spread of malicious software ("malware") between devices, potentially infecting our environment causing financial cost and loss of productivity. In

order to mitigate these risks, we restrict the use of removable media via this policy and via technical controls.

Where it is necessary to use removable media, for example to move data from specific equipment, you should endeavour to use encrypted removable media. Regardless, wherever possible, removable media should be antivirus scanned immediately **each time** it is connected to one of our devices.

Removable media should only be used as a temporary storage location for data. The removable media should **not** be the only copy of the data.

Use of removable media should be avoided wherever possible. If there is a need to exchange data, consider the use of the Council's provided cloud storage solutions.

When an item of removable media ends its usable life, is damaged, or fails it must be disposed of securely. Seek advice from the Clerk.

In extreme circumstances, the use of non-encrypted media may be permitted by agreement with the Clerk who can provide further advice.

Removable media from third parties

Our default position is that third parties should transfer data to us via cloud platforms, for example OneDrive, SharePoint or Google Drive. Where a third party cannot do so, the use of removable media may be permitted, however, it should be antivirus scanned immediately after connection.

If you find removable media, for example a memory stick dropped in the car park or left in a public area, you **must not** connect it to our equipment. This is a common way for attackers to gain access to or infect organisations.

Use of cloud storage solutions

We provide a cloud environment via Microsoft 365, including *Microsoft OneDrive for Business* and *SharePoint*. These are the only permitted cloud storage solutions for our data. You should not use Google Drive, Dropbox, or similar, without express written permission from the Clerk. This is because our environment has been configured in a way that meets our requirements.

You are encouraged **not** to store documents or attachments in email for extended periods of time. If a file is needed it should be uploaded to OneDrive / SharePoint or emailed to the office to be uploaded as soon as possible. Your email mailbox should be considered **temporary** storage.

Bring Your Own Device (BYOD) and personal devices

We permit the use of personal devices, such as laptops, tablets and smartphones, to access your provided email account. You must ensure your device is protected with a PIN code or biometrics. You may not download any attachments or store our data on your device for long periods, so any files you download, e.g. to review an attachment, must be deleted afterwards. We reserve the right to deploy technical controls to your device, for example mandating a PIN code. This does not give us access to your data.

Bearsted Parish Council

Data sharing

Where it is necessary to share data with third parties it is necessary for a *data sharing agreement* to exist between our two organisations. It is expected that the third party will have a data handling policy that provides at least the same level of protection as our own. Sharing agreements should have the approval of the Clerk.

From time to time it may be necessary to share data as a one off, or in an ad hoc fashion. You should seek approval from the data subject or the Clerk before any sharing takes place, and the Clerk will consider the implications of sharing the requested data, where appropriate.

Once sharing is agreed it will be performed via one of our approved methods. Our preferred methods are via *OneDrive for Business*, *SharePoint or email, as appropriate*.

Breaching this policy

We acknowledge that accidents happen, and sometimes this policy will be breached due to a genuine mistake. In these cases, you must report the situation to the Clerk as soon as possible, providing as much detail as you can. We will then work to contain the breach.

Where staff or Members intentionally breach this policy, the organisation may follow its other policies such as the Disciplinary Policy or Code of Conduct. Note that in serious cases, an intentional breach may be considered gross misconduct, potentially leading to termination of employment.

Interaction with other policies, laws, and frameworks

It may be necessary for you to also follow additional policies, laws, and frameworks that overlap with this Data Handling Policy. Where this is the case, you should discuss any overlaps and conflicts with the Clerk.
Note compliance with law will prevail over this policy.

Policy review

This policy will be reviewed annually, or when there is a significant change in either the law or our operating procedures.