BUXHALL PARISH COUNCIL

BRING YOUR OWN DEVICE POLICY (BYOD)

Document Control		
Date adopted	13 03 2023	Minute ref: 130323/53
Review date	March 2023	

Buxhall Parish Council (BPC) recognises the benefits that can be achieved by allowing Councillors to use their own electronic devices for Council business, whether that is at home, or at meetings. Such devices include laptops, smart phones and tablets, and the practice is commonly known as 'bring your own device' or BYOD. UPC is committed to supporting Councillors in this practice.

The use of such devices to create and process Council information and data creates issues that need to be addressed, particularly in the area of information security.

The Parish Council must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering Councillors to ensure that they protect their own personal information.

Responsibility of Councillors

Individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:

- Familiarise themselves with their device and its security features so that they can ensure the safety of Council information (as well as their own information)
- Invoke the relevant security features
- Maintain the device themselves ensuring it is regularly patched and upgraded
- Ensure that the device is only used in line with the values in the Code of Conduct (Suffolk) and the Nolan Principles.
- The Parish Council cannot take responsibility for supporting devices it does not provide.

Councillors using BYOD must take all reasonable steps to:

- Prevent theft and loss of data
- Keep information confidential where appropriate
- Maintain the integrity of data and information
- Take responsibility for any software they download onto their device

Councillors using BYOD must:

- Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device
- Where it is essential that information belonging to the Council is held on a personal device it should be deleted as soon as possible once it is no longer required. This includes information contained within emails
- Ensure that relevant information is copied back onto Council's systems and manage any potential data integrity issues with existing information
- Report the loss of any device containing Council data (including email) to the Clerk
- Be aware of any Data Protection issues and ensure personal data is handled appropriately.
- Report any security breach immediately to the Clerk
- Ensure that no Council information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party
- Ensure they immediately delete all council data from their personal devices once they have left the Council

Monitoring and Access

The Council will not routinely monitor personal devices. However it does reserve the right to:

- prevent access to a particular device from either a wired or wireless network or both
- take all necessary and appropriate steps to retrieve information owned by the Council

Data Protection and BYOD

The Council must process 'personal data' i.e. data about identifiable living individuals in accordance with the Data Protection Act 2018 and the General Data Protection Regulations. Sensitive personal data is information that relates to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (mental or physical) or details of criminal offences. This category of information should be handled with a higher degree of protection at all times.

The Council, in line with guidance from the Information Commissioner's Office on BYOD, recognises that there are inherent risks in using personal devices to hold personal data. Therefore, Councillors must follow the guidance in this document when considering using BYOD to process personal data.

A breach of the Data Protection Act 2018 or the GDPR can lead to the Council being fined. Any Councillor found to have deliberately breached the Act or the Regulations may be subject to disciplinary measures or even a criminal prosecution.