INFORMATION TECHNOLOGY POLICY GUIDELINES

Bishopston CC

Each council will have their own IT provision and a 'fit-for-all' policy is not possible. Some small Parish councils will have minimal equipment whilst others may multiple devices linked to a server. These guidelines are designed to help councils consider some of the factors that may need to go into a policy. Those councils with external IT providers should ensure any policy reflects the current practice.

The purpose of an IT policy is to set out the parameters on how council staff should use the technology that you provide them with in order to do their job.

A clear policy will also help to raise awareness of the risks associated with using IT and can protect the council from loss of data. Councils will need to take a view on whether staff are permitted to use IT equipment for personal use (i.e. accessing webmail or online shopping at lunchtimes). The policy needs to clarify acceptable and non-acceptable use and what will happen if the policy is breached.

As an employer you have the right to monitor work use of IT equipment provided you have a legitimate reason and that you tell staff that you might do this.

When drafting your IT Policy, use the following questions/points to guide the areas to cover:

- Who does the policy apply to?

- What communications and IT equipment does the policy cover? For example, computers, internet access, remote access connections, email servers, file storage, webmail, smart phones, telephones, website, mobile phones etc.

- Who is responsible for monitoring and reviewing the policy? Ideally there should be one individual with overall responsibility. This person should help staff understand the policy and enforce it.

- Related policies – what other policies do you have which set out standards of behaviour that apply equally to online behaviour? Examples may include Disciplinary Rules, Data Protection Policy, Equality and Diversity Policy etc.

- Monitoring – Do you monitor how staff use the internet, email or work telephones? Employers are able to do so in particular circumstances although this would need to be properly communicated in the policy. If you have CCTV then you will need a separate policy to explain how you store and use the records. If you allow staff to use equipment for personal use, staff should be made aware that you may still monitor usage.

· Passwords – What are your rules around passwords and accessing IT systems? Can they be disclosed? If so, to whom? What happens if you need to access another

employees' computer system (for example if they are off sick)? Do you transmit confidential or personal sensitive information and if so, what are your password protection protocols? What length and form must passwords be? What should an employee do if they think someone else knows their password? If password protected documents are emailed, how should the password be notified?

· Computer usage – clarify that computers should be shut down at the end of every day. Should employees log out of their systems when they move away from their desks? Should documents be saved in a location accessible for back up? What precautions are needed for areas with public access?

· Do you allow individuals to bring in their own IT equipment and use then for work purposes? If you do, are there restrictions or specific requirements?

· Data Protection – ensure you reference the requirements when processing personal data in accordance with the six data protection principles. Your policy should explain your rules on collecting, storing, retaining, using disclosing and disposing of personal information. It should also set out how the council protects data and prevents unauthorised or unlawful processing or disclosure.

· Mobile phone texting – is this appropriate for work issues? Who to (members of the public, suppliers, LA's etc)? Should abbreviations be avoided? Text messages from the council are treated in the same way as emails, for example they must not contain illegal or discriminatory content.

· Email: What rules do you need to consider with regard to email communication? Email is sometimes seen as a casual way to communicate and this may present a reputational risk. Clear rules on email may also prevent staff from inadvertently entering into an agreement with a supplier.

· Internet – what can the internet at work be used for and what can't it be used for? Is a firewall in place? What does this mean for staff? What limits are there on accessing chat rooms, messaging services, blogs etc from work IT and communication systems?

· Software – what rules and controls are in place for downloading software onto work machines.

· Training – consider including a few words on what training and support exists for staff with regards to information security. For example, do you train staff as part of their induction on the risks of email security?

· Misuse – be clear that misuse of IT facilities can potentially result in disciplinary proceedings. What constitutes misuse? Examples could include not adhering to the policy; attempting to discover a user's password; using the computer systems to act abusively; attempting to circumvent the network's security; knowingly running and installing programmes intended to damage the computer systems; deliberately wasting computer resources; leaving laptops unattended in a public place etc.