# **Information technology POLICY GUIDELINES**

The purpose of an IT policy is to set out the parameters on how staff should use the technology that your charity provides 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 charity from loss of data. Charities 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, mobile phones etc.
* Who is responsible for monitoring and reviewing the policy? Ideally there should be one individual with overall responsibility. The policy should require managers to 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 Codes of Conduct, Disciplinary Rules, Data Protection Policy, Equality and Diversity Policy etc.
* Monitoring – Do you monitor how staff use the internet, email or work telephones? When and how do you do so? 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 your policy will need 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 these be disclosed to senior staff? 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 – should computers be shut down at the end of every day? Does this include screens? 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?
* Do you allow individuals to bring in their own IT equipment (such as USB sticks) and use them 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 charity protects data and prevents unauthorised or unlawful processing or disclosure.
* Mobile phone texting – is this appropriate for work issues? Who to (funders, suppliers, external stakeholders etc)? Should abbreviations be avoided? Text messages from the charity 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 employees? Can employees subscribe to chat rooms, messaging services, live streaming, 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 – will misuse of IT facilities 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.

The HR Services Partnership can help you draft a policy or procedure which is specific to your organisation. As an NCVO Trusted Supplier we offer preferential rates for members of NCVO.