IT POLICY FOR <Organisation>

2021

1. The aim of the IT policy

The Organisation is committed to maintain up to date, safe IT equipment, used in accordance with all relevant legislation, notably those relating to data protection, human rights and freedom of information. This policy aims to define a code of conduct which safeguards the security and confidentiality of information held within the Organisation’s electronic systems.

The company's hardware and software, including any work phones and e-mail facilities, may only be used for business purposes except in the circumstances outlined below.

The policy applies to all staff, trustees and volunteers. Failure to observe procedures may be regarded as misconduct, and will be dealt with according to the Organisation’s normal disciplinary procedure.

1. Key principles

Our data will be made available solely to those who have a legitimate need for access to it.

It is the responsibility of all individuals who have been granted access to information to handle it appropriately.

Any user id issued to you is unique and personal. It must not be disclosed to any other individual including other staff at the Organisation. Staff are expected to remember their password, to change it every year. Passwords must be changed immediately if there is any suspicion that it may have been compromised. All passwords must be strong passwords: at least seven characters, using a mixture of uppercase, lowercase, numbers and punctuation. It’s best not to be re-using the same password within a two-year period.   
   
Each member of staff will also be assigned a unique email address for his or her individual use and some members may also be given authorisation to use one or more generic email addresses. Staff must never use email addresses assigned to others.

1. Computer standards and BYOD

All user accounts used for day-to-day tasks must be personal standard accounts. Shared accounts are not acceptable. Administrator accounts should be reserved solely for installing new software and performing updates. An Organisation-approved antivirus must be installed on all computers used for business purposes, including personal devices used to access the Organisation’s data. All software on the computer, including the antivirus and the operating system, must be kept up to date at all time. Operating system updates must be installed within two weeks of their release. Antivirus definitions must be installed within one day of release.

All staff, trustees and volunteers are allowed to use their own personal devices for work purposes, but those personal devices must comply with the standards set out in this policy, and the Organisation reserves the right to revoke the policy for any or all members of staff.

1. Email and IT usage monitoring

The Organisation reserves the right to monitor staff’s emails and use of the internet, both during routine audits or random spot checks of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected.

The Organisation will only monitor email and internet use where we have a lawful basis for

doing so.