Somerset West and Taunton

Volunteer Data Protection Policy

Introduction

Somerset West and Taunton Council collect, hold and use personal data in order to conduct its business. The Council has a statutory duty under UK law to safeguard this information.

This policy aims to reduce the likelihood and impact of any data breaches. There are a variety of risks, some of which can result in the Information Commissioner's Office (ICO) imposing significant fines.

You and Data Protection

You must only access personal data, client records, files and folders for the reason that it was given (the purpose) or for statutory requirements. Unauthorised access is a criminal offence. Your Volunteer Manager will make sure you are aware of the information you should be accessing and how to use it for your role. You should not be given access to information outside the remit of your role.

Releasing information to safeguard people at immediate risk of harm is allowed under Data Protection.

All members of the public and employees, as data subjects, have statutory rights including the right to know what information we hold and the right to be forgotten where a data subject can request that we delete records we hold about them unless it is required to be kept by law.

Depending on your role, you must complete the Data Protection E-Learning modules and any ongoing Data Protection training as required.

Reporting

If you are aware that you, or someone else, has disclosed personal or sensitive data, to someone who did not have permission or authority to receive that information, you must report it immediately to your Volunteer Manager or other Council staff member.

Any loss or theft of data should also be immediately reported.

Your Volunteer Manager must report it to the Data Protection Officer as soon as possible as there is a **72 hour** deadline to disclose reportable breaches to the ICO.

Technology

The Council must protect personal data across a wide range of technologies and in a variety of environments.

If you have been provided a Corporate device for use outside the [[insert volunteer project or opportunity name here] (for example if you are providing assistance remotely), all the personal data held by it will be encrypted. You will be trained to ensure that data is kept securely and that your use of the device is appropriate and secure.

Phone calls (including mobile) and virtual telephony service (I.e Microsoft teams)

When making a phone call or using other virtual telephony services for calls of a personal and sensitive nature:

- Ensure you cannot be overheard by anyone not directly concerned with the call.
- Before sharing personal data ensure the other party is a trusted individual, if necessary, call them back to confirm their identity.
- Don't leave voice or answer machine messages in case they are picked up by someone other than the intended person
- Outside the office ensure you cannot be overheard by anyone, where this is not possible use only first names and try and avoid discussing personal and sensitive issues.

Video Recordings and photographs

Video recordings and photographs that can be identified as individuals are defined as personal data. Ensure that any service users, volunteers, or employees are fully informed if you are taking photographs or making videos.

The data subjects must be told what the information will be used for, why it has been collected, if it will be shared with anyone and how it will be kept before it is destroyed.

Policy Compliance

If you are found to have breached this policy, you may no longer be able to volunteer at a [insert volunteer project or opportunity name here] or any other Council service

Where it is considered that a criminal offence has potentially been committed, the Council will consider the need to refer the matter to the police.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your Volunteer Manager.

The council's full Data Protection Policy can be accessed via…