St Ives Town Council
TWINNED WITH STADTALLENDORF
TOWN CLERK: Alison Melnyczuk BA (Hons) FILCM
Town Hall, Market Hill, The Old Riverport, St Ives, Cambridgeshire PE27 5AL
Telephone: 01480 388929
email: clerk@stivestowncouncil.gov.uk

DATA PROTECTION POLICY

1. Introduction

1.1 St Ives Town Council (hereafter known as SITC) needs to keep certain information about its employees, volunteers, members and service users to allow it to monitor performance, achievements, health and safety and other statutory requirements, as well as to send information of interest to them. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, SITC must comply with the eight Data Protection Principles, which are set out in the Data Protection Act 1998. In summary these state that personal data shall:

- be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- be adequate, relevant and not excessive for those purposes
- be accurate and kept up to date
- not be kept for longer than is necessary for that purpose (see Retention of Records Policy)
- be processed in accordance with the data subject's rights
- be kept safe from unauthorised access, accidental loss or destruction and
- not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

1.2 Important Note: The Data Protection Act 1998 extends the scope of legislation to include written and printed etc. material, not just the electronic data.
SITC and all of its staff, or others who process or use any personal information, must ensure that they follow these principles at all times. In order to ensure that this happens, SITC has developed this Data Protection Policy and also had a Retention of Records Policy.

2. What is defined as personal data?

2.1 Personal data is defined in the Act, at Section 1(1), as follows:
"data which relates to a living individual who can be identified: from those data; or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual".

2.2 However the Information Commissioner would advise caution in working only to this limited definition.

3. Status of the policy

3.1 This policy is incorporated in SITC formal contract of employment. Infringement of the requirements of this policy may result in disciplinary action being taken. If any SITC staff, volunteers, members or service providers consider that this Policy has not been followed, in respect of personal data about themselves, they should raise the matter initially with the designated Data Controller. If the matter is not resolved it should be raised as a formal grievance.

4. Responsibilities of staff

4.1 All staff are responsible for: checking that any information that they provide to SITC in connection with their employment is accurate and up to date informing SITC of any changes to information which they have provided, e.g. changes of address and informing SITC of any errors or changes in staff information.

4.2 If and when, as part of their responsibilities, staff collect information (i.e. personal information, opinions about ability, or details of personal circumstances) about other people or members, they must comply with any guidelines which may be published. In particular, they must seek the permission of the Data Controller for their proposed information collection and uses.

4.3 The Town Clerk has overall responsibility and is responsible for monitoring the steps taken to ensure that the Act and this Policy are complied with. Particular care must be taken when work is being undertaken externally or when an existing body of material is being brought within SITC for the first time.

5. Data security

5.1 All staff are responsible for ensuring that:

. Any personal data, which they hold, or for which they are responsible, is kept securely, for example:

. Kept in a locked filing cabinet;

. In a locked drawer;

. If it is computerised, be password protected

. If computerised, then the computer itself is kept in suitably secure conditions.

. Data should not be stored on the hard drives of desktop personal computers but on the networked storage facilities provided.

. Where it is necessary to store information on laptop computers (or off-site) then the machine must at all times be maintained physically secure. Where the data is particularly sensitive, consideration must be given to the adoption of additional security measures which would protect the information in the event of the loss or theft of the computer. Care must be taken to ensure that data is frequently transferred to network storage and that discrepancies are not allowed to arise.

- Where information is to be gathered through, or used on, a website then appropriate measures must be in place to control access and prevent unauthorised disclosure.

5.2 Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. (With the exception of vulnerable adults and children or others at risk)

5.3 Advice on the collection, retention and secure storage of information may be obtained from the Data Controller.

5.4 Staff should note that unauthorised disclosure is a breach of the Data Protection Act and may result in disciplinary action. In some cases it may be considered as gross misconduct. It may also result in a personal liability for the individual staff member.

6. Rights to access information, *Subject Access Request* (S.A.R.s)

6.1 Employees and other users / members of SITC have the right to access any personal data that is being kept about them either on computer or in other types of files. Should any person wish to exercise this right they should contact the Data Protection Controller.

6.2 In order to gain access, a request should be made in writing to the Data Protection Controller. SITC reserves the right to make a charge of up to £10 on each occasion that access is requested.

6.3 SITC aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days.

7. Subject consent

7.1 In many cases, SITC can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to SITC processing some specified classes of personal data is a condition of employment for staff. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974.

7.2 Therefore, all prospective staff will be asked to consent to their data being processed when an offer of employment is made.

8. Processing sensitive information

8.1 Sometimes it is necessary to process sensitive information about a person such as race, gender or family details. This is done to ensure that can operate SITC policies on matters such as sick pay or equal opportunities. SITC may also ask for information about particular health needs or disabilities. SITC will only use such information in the protection of the health and safety of the individual, but will need consent to process - for example, in the event of a medical emergency.

Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, employees and others affected will be asked to give express consent for SITC to do this.

9. The Data Controller

9.1 The designated Data Controller will deal with the implementation of the agreed policy and day to day matters.

9.2 SITC designated Data Controller is the Town Clerk.

10. Retention of data

10.1 SITC will keep some forms of information longer than others.
SITC will need to keep central personnel records for 6 years after employment ceases. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. Retention of all other documents and paperwork are detailed in the Retention of Records Policy.

11. Conclusion

11.1 Compliance with the Data Protection Act 1998 is the responsibility of all staff, volunteers and members of SITC. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to SITC facilities being withdrawn, or even a criminal prosecution.

11.2 Any questions or concerns about the interpretation or operation of this Policy should be taken up with the Data Controller.