



Southampton Voluntary Services

Southampton Voluntary Services

Data & Confidentiality Policy

Amendment History

Version 1998, Issue 1.0, December 1998	
Version 2005, Issue 1.1, September 2004	
Version 2007, Issue 1.2, February 2007	<ul style="list-style-type: none">○ Storing, Sensitive & Access to Information○ Reference to the FOIA○ SVS information/records
Version 2014, Issue 1.3, January 2014	Reviewed

Reviewer

**Deputy Chief Executive,
Senior Administrator**

Owner and Authorised by:

**Chief Executive and
Executive Committee**

Introduction

SVS has access to information concerning many groups and individuals in the city and it is therefore imperative that the strictest confidentiality is maintained at all times. Information belongs to the person or agency entrusting it to a member of staff or volunteer of SVS. Any information passed on outside of SVS will only be given with the express permission of the person or body which supplied the information unless we are legally obliged to disclose it.

SVS has notified the Data Protection Unit under the Data Protection Act and our Deputy Chief Executive is the appointed Data Controller. We endeavour to ensure that all information is stored under their guidelines.

The Data Protection Principles

The Act requires that eight data protection principles be followed in the handling of personal data. These are that personal data must be:

Fairly and lawfully processed.

Processed for limited purposes and not in any manner incompatible with those purposes.

Adequate, relevant and not excessive.

Accurate.

Not kept for longer than is necessary.

Processed in accordance with the data subject's rights.

Secure.

Not transferred between countries without adequate protection.

We are committed to following these principles and will be open and transparent about what the data will be used for. We will process personal data about you only as far as is necessary for the purpose of managing the Organisation's business in which you are employed, volunteer or any client details that you may hold. Unless you expressly authorise its disclosure, your personal data will not be disclosed to anyone else other than authorised employees, those who provide relevant services to the Organisation (such as advisers and payroll administrators), regulatory authorities, potential or future employers, governmental or quasi-governmental organisations. We will only obtain personal data about you that it requires for the purpose of managing its business and dealing with you as an employee.

We will take all reasonable steps to ensure that the personal data it processes is accurate and not excessive. Personal data will be retained as necessary during the course of your employment and records will be retained for up to six years after you leave the organisation's employment in case legal proceedings arise during that period. Different categories of data may be retained for different periods of time depending on legal, operational and financial requirements. Data will only be retained for a period of longer than six years if it is material to ongoing legal proceedings or it should otherwise be retained in the interests of the organisation after that period.

Manual personal data, such as personnel files, is stored in locked filing cabinets. Personal data held on computer is stored confidentially by means of password protection. We have a network of back-up procedures to ensure that data on computers cannot accidentally be lost or destroyed.

Consent to Processing

It is a requirement under the Act that you consent to us processing personal data about you. Some data is referred to in the Act as 'sensitive' personal data. This means personal data comprising information relating to:

- Race or ethnic origin.
- Political opinions
- Trade Union membership.
- Religious or other beliefs.
- Physical or mental health or condition.
- Sexual life.
- Criminal offences both committed and alleged.

It therefore follows that some of the personal information that we will have to process about you will be sensitive personal data, for example, information about your physical or mental health in order to monitor sick leave and take decisions about your fitness for work and your racial or ethnic origin, or religious or similar beliefs, in order to monitor compliance with equal opportunities legislation.

It is a term of your contract of employment that you expressly consent to the organisation collecting, retaining and processing data including sensitive personal data about you for legal, personnel, administrative and management purposes. This data includes but is not limited to your name and address, salary details, bank details, date of birth, age, sex, ethnic origin, next of kin, sickness records, medical reports and details of criminal convictions. This information will only be used in order that we can monitor our compliance with the law and best practice in areas such as equal opportunity, pay and benefits, administration, performance appraisal and disciplinary matters. If your personal information changes, you should let us know so that our records can be updated.

Unless you give this consent it is not necessarily lawful for us to process the personal data that we need in order to keep the necessary records about your employment and, therefore, it is not possible for us to meet the needs of running our business in relation to your employment without your consent.

Your Rights to Access Personal Information

Under the Act, you have the right to find out what personal information we hold about you, and to ask for a copy of that personal data. You also have the right to demand that any inaccurate data be corrected or removed and to seek compensation where you suffer damage or distress as a result of any breach of the Act by the Organisation.

You have the right on request to:

Be told by the organisation whether and for what purpose personal data about you is being processed.

Be given a description of the personal data concerned and the recipients to whom it is or may be disclosed.

Have communicated in an intelligible form the personal data concerned, and any information available to the organisation as to the source of the data.

Be informed in certain circumstances of the logic involved in computerised decision-making.

A request for access to any personal data that relates to you should be made in writing to your Manager and should specify what personal data your request relates to. You can use our Personal Data Request Form for this purpose, a copy of which can be obtained from HR. We reserve the right to charge a fee of up to £10.00 or such higher amount as permitted by law from time to time before access can be granted. The organisation also reserves the right to make further enquiries of you in order to satisfy ourselves as to your identity and to help us locate the personal data that you have requested.

Upon receipt of a request it is our policy to provide copies of all personal data that we are obliged to disclose within 40 days of your request being received. We consider that if a period of less than one year has elapsed since any previous request for access to your personal data was complied with, it is not reasonable to expect us to be obliged to comply with a further request unless there are exceptional circumstances.

Should you wish to bring any inaccuracy in disclosed data to our attention you must do so in writing to your Line Manager. It is the organisation's policy to ensure that all data is as accurate as possible and all necessary steps will be taken to ensure that this is the case and to rectify any inaccuracies.

Where we have requested a reference in confidence from a referee and that reference has been given on terms that it is confidential and that the person giving it wishes that it should not to be disclosed to you, it's our policy that it would normally be unreasonable to disclose such a reference to you unless the consent of the person who gave the reference is first obtained.

We reserve the right not to disclose to you any management forecasts or management planning documentation, including documents setting out the plans for your future development and progress.

Your Obligations in Relation to Personal Information

You must comply with the following guidelines at all times:

Do not give out confidential personal information except to the data subject. In particular, it should not be given to someone, either accidentally or otherwise, from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this.

Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.

Only transmit personal information between locations by fax or email if a secure network is in place, for example, a confidential fax machine or encryption is used for email.

If you receive a request for personal information about another employee, you should forward this to your Manager.

Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected.

Appendix A
Statutory Retention Periods

Record	Statutory Retention Period	Statutory Authority
Accounting records	6 years	Section 221 of the Companies Act 1985
Banking records Cheques, bills of exchange and other negotiable instruments, bank statements Instructions to banks	3 years for ltd Companies 6 years after ceasing to be effective	
Payroll		
Wages/ salary records (also overtime, bonuses expenses)	6 years	Taxes Management Act 1970
Income tax and NI returns	Not less than 3 years after the end of the financial year to which they relate	The Income Tax (employments) Regulations 1993
Statutory Maternity Pay records, calculations, certificates (Mat B1's) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986
Statutory Sick pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982
Health and Safety		
Accident books, accident records/reports	3 years after the date of the last entry	The reporting of injuries, diseases and dangerous occurrences Regulations 1995
Records relating to children	Until the child reaches the age of 21	Limitation Act 1980
Records relating to events notifiable under the Retirement Benefits Schemes. Regulations 1995, records concerning decisions to allow retirement due to incapacity, pension	6 years from the end of the scheme year in which the event took place, or the date upon which the accounts/reports were signed/completed	The retirement benefits Schemes (information powers) Regulations 1995

accounts and associated documents		
-----------------------------------	--	--

Recommended retention periods for all other information

Record	Recommended retention period
Personnel Information	
Application forms and interview notes	6 months after appointment of successful candidate
Parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance
Pensioners records	12 years after benefit ceases
Personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases
Redundancy details, calculations of payments, refunds, notification to the secretary of state	6 years from the date of redundancy
Time sheets	2 years after audit