Turn2us

Data Protection Policy

Contents

1. Policy Statement

1.1 Turn2us recognises that there is a general expectation from its employees, service users and other stakeholders that any personal information the organisation holds about them will be stored and handled to the highest standards of confidentiality and integrity. The organisation actively promotes awareness of and compliance with the Data Protection Act 1998 ('DPA 1998') as a code of practice for good information management and handling. The requirements of the DPA 1998 are set out below for the guidance of trustees, employees and volunteers.

2. The Data Protection Act (DPA) 1998 - Definitions

2.1 The Data Protection Act 1998 ('DPA 1998') sets out the legal requirements and rules for processing personal data. Key terms are written in **bold text** on the first occasion they are used.

2.2 The term **'personal data'** refers to information about identifiable living individuals. Personal data include a significant amount of information stored in paper records as well as information held on computers. A '**data subject'** is the individual who is the subject of the personal data.

2.3 Those who decide how and why personal data are processed are termed **'data controllers'**. Data controllers must comply with the rules of good information handling that are set out in eight **'data protection principles' – see paragraph 6.1**. Other additional requirements of the DPA 1998 are explained below.

2.4 Personal data covers both **facts and opinions** about an individual. It also includes information regarding the **intentions of the data controller** towards the individual.

3. Paper Files

3.1 The Data Protection Act 1998 covers all personal data that are recorded as part of a **'relevant filing system'**. This is a set of information in which the records are structured by either reference to individuals or by reference to criteria relating to individuals, so that **'***specific information relating to a particular individual is readily accessible'*. This definition means that a significant proportion of the information held in Turn2us's paper files falls within the scope of the DPA 1998 (e.g. information about service users).

4. Notification to the Information Commissioner

4.1 The DPA 1998 requires every data controller who is processing personal data to notify the Information Commissioner unless they are exempt – see paragraph 4.3 below. The Information Commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller and a general description of the reasons why processing of personal data by a data controller is being undertaken. Members of the public can consult the register to find out what processing of personal data is being carried out by a particular data controller.

4.2 '**Notification'** is the process by which a data controller's details are added to the register. Notifications are renewable annually. If a new data processing system is introduced or an existing one altered then a new notification must be sent. Organisations are only allowed one data registry entry.

4.3 There are a limited number of **exemptions** from the need to notify. These include certain voluntary organisations (see below), the processing of personal data for personal, family or household affairs, data controllers who only process personal data for the maintenance of a public register, and data controllers who only process information in connection with their business for staff administration, advertising, marketing and public relations, or accounts and records.

4.4 The exemptions for voluntary organisations basically apply to societies and clubs, which are exempt if their data processing is limited to one of the following purposes:

- 'Establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are either members of the body or association or have regular contact with it - for small clubs, voluntary organisations, church administration and some charities
- The data subjects are restricted to 'past, existing or prospective members', or those who have regular contact with the organisation
- Any person whose personal data is necessary for an exempt purpose
- Where disclosure of the personal data to a third party is necessary for an exempt purpose
- Where the personal data are not kept.

4.5 A self-assessment form to establish whether or not notification is required can be found on the Information Commissioner's website:
http://forms.informationcommissioner.gov.uk/notify/self/question1.html

5. Application of the DPA 98 Requirements to Turn2us

5.1 Turn2us is required to notify because the charity handles and stores a significant amount of personal data about service users and may need to exchange this information on a confidential basis with referrals agencies. Turn2us must notify the Information Commissioner of the purposes for which personal data are held, and the organisation's name will be placed on a public register.

5.2 All those associated with the organisation's management – employees, committee members and volunteers - must comply with the DPA 1998 requirements in respect of the storage and handling of personal data at all times.

5.3 Turn2us has nominated its IT Director as the Data Controller for Turn2us. When providing a notification to the Information Commissioner, the Data Controller will provide the following information:

- A description of the personal data to be processed and the category(ies) of data subject to which the data relate
- A description of the purposes for which the data are to be processed
- A description of any recipient(s) to whom the data controller intends to disclose the data and
- A general description of the security measures to be taken to ensure that personal data are protected.

5.4 In order to ensure that the organisation is complying with this requirement, every staff member, trustee or volunteer who has responsibility for or holds personal data, either on a computer system or any other 'relevant filing system', should establish whether or not the system contains personal data. If it does, then a 'Personal Data Held by Turn2us' form must be completed providing the details set out above.

5.5 The data controller will check that the information on the form is correct, and then create a summary of all the personal data that are held across the organisation. The summary will form the basis of the notification to the Information Commissioner.

5.6 The Notification Form can be downloaded from the Information Commissioner's website: http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx, printed off and then sent to the Information Commissioner's Notification Department once it has been completed. A fee is payable.

6. The Rules of Good Information Handling – The Eight Principles

6.1 The eight principles of good information handling are as follows.

- Personal data must be obtained and processed fairly and lawfully
- Personal data must only be held for specified and lawful purposes and not in any manner incompatible with those purposes. The purposes for which personal data are held is described in Turn2us's entry in the Register, and information may not be held for another purpose
- Personal data must be adequate, relevant and not excessive in relation to the purposes for which it is held
- Personal data must be accurate and, where necessary, kept up to date
- Personal data must not be kept for longer than is necessary for the purposes covered by the registration
- Personal data must be processed in accordance with the data subject's rights. This means that the data will be made accessible to the person concerned and where appropriate the information will be corrected or erased
- There must be appropriate security measures in place to:
  - Prevent unauthorised access to or alteration, disclosure or destruction of the personal information and
  - Prevent accidental loss or destruction of the personal information
- Personal data should not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

7. Processing Personal Data

7.1 The action of 'Processing' is broadly defined and takes place when any operation or set of operations is carried out on or using personal data. The DPA 1998 requires that personal data are 'processed fairly and lawfully'.

7.2 Personal data will not be considered to be processed fairly unless the following conditions are met:

- The processing is necessary to carry out public functions
- The processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

7.3 Turn2us will process personal data fairly and lawfully by ensuring that the above conditions are met whenever it processes personal information.

8. Processing Sensitive Data

8.1 The Data Protection Act 1998 makes specific provision for sensitive personal data. Sensitive data includes racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; personal health; sex life; criminal proceedings or convictions.

8.2 Sensitive data can only be processed under strict conditions including:

- Having the explicit consent of the individual data subject
- Being required by law to process the data for employment purposes
- The need to process information in order to protect the vital interests of the data subject or another
- Dealing with the administration of justice or legal proceedings.

9. The Individual's Rights

9.1 The right of subject access

9.1.1 The DPA 1998 allows individuals to find out what information is held about themselves on computers and in some paper records. This is known as the '**right of subject access'**. In addition to the right to receive a copy of all the personal data held about the individual, the subject is also entitled to be told that the data controller or someone on the data controller's behalf is processing data about them, to be given a description of the personal data, the purposes for which the data are being processed and a description of those to whom the data may be disclosed. The subject is also entitled to receive information about the sources of the data and where decisions are made by '**fully automated'** means, to receive a statement of the logic of the decision-making software.

9.2 Right to prevent processing likely to cause damage or distress

9.2.1 A data subject can ask a data controller to stop processing or request that they do not start processing information relating to them where it is causing or is likely to cause substantial unwarranted damage or distress to themselves or anyone else. However, this right is not available in all cases and data controllers do not always have to comply with the request.

9.3 Right to prevent processing for the purposes of direct marketing

9.3.1 A data subject can ask a data controller to stop or not to start processing data relating to them for direct marketing purposes. This is an absolute right.

9.3.2 A data subject can ask a data controller to ensure that no decision which significantly affects them is based solely on processing their personal data by automatic means.

9.4 The Right to Compensation

9.4.1 A data subject can claim compensation from a data controller for damage or distress caused by any breach of the DPA 1998. Compensation for distress alone can only be claimed in limited circumstances.

9.5 The Right to take action to rectify, block, erase and destroy

9.5.1 The DPA 1998 allows individuals to apply to the Courts to order a data controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.

10. Criminal Offences

10.1 It is a criminal offence if data controllers do not notify the Information Commissioner either of the processing of personal data that is taking place, or of any changes that have been made to that processing. It is also a criminal offence to:

- Obtain or disclose personal data in breach of the notification or without the permission of the data controller
- Obtain, disclose, sell or advertise for sale or bring about the disclosure of personal information without the consent of the data controller
- Access personal data or disclose it without proper authorisation - this covers unauthorised access to and disclosure of personal data.

10.2 Unless one of the limited statutory exceptions apply, it is an offence for a person to ask another person to make a subject data access request in order to obtain personal data about that person for specified purposes, including as a precondition to employment.

11. Dealing with Requests from within Turn2us

11.1 The organisation may ‘use’ (as opposed to ‘share’) information internally provided it is for legitimate purposes in pursuance of the organisation’s normal business. In addition, where information is sought by one team, section or department from another, this should be restricted to the specific details required and general access to computer systems or paper records should not be given.

12. Dealing with Requests for Information from outside bodies

12.1 Requests from the Police

12.1.1 Any requests for disclosure of personal data received from the police should be accompanied by a written explanation. This explanation should inform Turn2us that the data required is an essential part of a criminal investigation. Where no such explanation is provided, the organisation should refuse to disclose the data requested until a valid written explanation is received.

12.2 Requests from Inland Revenue and Customs and Excise (VAT) Inspectors

12.2.1 These should be treated in the same way as those from the police. Inland Revenue and Customs and Excise VAT Inspectors will often state that in addition to their powers under the DPA 1998, they are also acting under their statutory powers. Before disclosing any personal data, employees should ask for a written explanation of these powers. Provision of a section number or paragraph number from a relevant Act of Parliament should be regarded as insufficient unless it is also accompanied by the relevant wording or some other form of explanation of the powers and the purposes for which the data are required.

12.3 Requests from Local Authorities or Government Departments

12.3.1 On receipt of a request for information from a local authority or government department, Turn2us's employees must establish the purpose for which the personal data are required (for example to tackle benefit fraud) and the legal authority under which the request is made. Staff should seek confirmation in writing that the data are essential to the investigation and that they will not be used for any other purposes.

13. Employment Issues

13.1 Turn2us will provide each employee with an annual statement of the relevant personal data held on the personnel computer system.

13.2 The organisation can refuse access to certain types of data including:

- Confidential references
- Data processed for management planning if disclosure would prejudice the conduct of the business
- Records of employer's intentions in employee negotiations.

14. Disclosure of Personal Information – Practical Guidance Notes for Employees

14.1 Employees should inform the data controller promptly of any changes in their personal information (e.g. address, telephone number, marital status).

14.2 Employees and others who have responsibilities for holding or using personal data should:

- Ensure that all systems are accurate, up to date and processed in accordance with the relevant notification
- Only disclose personal data to assist them in carrying out their job
- Only disclose personal data to those authorised by the registration
- Not divulge personal or sensitive data unless they are sure it is in accordance with the data protection notification and treat all personal data with care
- Check the identities of people before disclosing information by telephone, e-mail, letter and before disclosing information in an interview
- Only disclose personal data to those people with a need and right to know
- Ensure that their personal security measures are adequate (e.g. secure the data on desks or in computers)
- Ensure that unauthorised staff, committee members or volunteers, service users or members of the public cannot read visual display screens - for this reason, do not leave screens unattended or 'logged in'
- Dispose of waste computer listings and printed matter as Confidential Waste
- Forward any subject access requests to the Data Controller in the first instance.

14.3 If in doubt about any aspect of the responsibility for holding or using personal data, employees should not disclose personal data and should seek advice from their line manager or the Data Controller.

15. The Freedom of Information Act 2000

15.1 If any data or information requested is not about a living individual (i.e. not personal data) but is in relation to a public authority, the provisions of the Freedom of Information Act 2000 apply. The Freedom of Information Act 2000 gives the public a general right of access to '**recorded'** information held by public authorities that is not personal data. However, some

records contain exempt information, which does not have to be disclosed when public authorities respond to requests for information. In total, there are twenty-three exemptions from the rights of access to information (e.g. information relating to national security, commercially sensitive information and confidential information).

15.2 Under the Freedom of Information Act 2000, public authorities generally have twenty working days to respond to requests for information.

15.3 Registered social landlords, housing support providers, voluntary and community organisations and charities are not public authorities. However a number of these organisations have adopted the principles of the Freedom of Information Act 2000 and its rights of access, subject to compliance with the Data Protection Act 1998.

15.4 At some time in the future, Turn2us may wish to consider whether or not to adopt the freedom of information principles, including adopting a publication scheme. A publication scheme is a guide to the types of information that the organisation routinely publishes, the format in which the information is available and how much it will charge for providing the information if there are any charges. The information is presented in the form of classes (categories) of information. For public authorities, the Information Commissioner may also approve model publication schemes for groups of similar bodies (e.g. schools).

Adopted: November 2009

Reviewed: April 2014

Review Date: April 2015

Policy Owner: Turn2us Director.

The following related policies should be read in conjunction with this policy:

- Code of Conduct
- Confidentiality Policy

PERSONAL DATA HELD BY TURN2US

Any staff member, trustee or volunteer who has responsibility for or holds personal data, either on a computer system or any other relevant filing system should complete this form and send it to the IT Director (Data Controller). The term 'personal data' refers to information about identifiable living individuals. The collation of this information is a requirement under the Data Protection Act 1998.

Name of data holder	
Name of computer system/filing system	
Description of data to be processed	
Category(ies) of data subject	
Purpose of data	
Recipients who may receive the data	
Security/Protection arrangements for the data	