10.1 – Data Protection & Confidentiality

Purpose and Scope

This policy covers the charity Elizabeth Finn Care ('EFC'), trading as Turn2us. It applies to all of the Turn2us's employees, contractors and agents including voluntary agents (hereafter referred to as 'Individuals'). This policy has two main purposes:

- To detail Turn2us' expectations regarding the handling of personal and sensitive data.
- To explain the information Turn2us holds on Individuals.

Turn2us actively promotes compliance with, and broad awareness of, the Data Protection Act 1998 ('DPA') as a code of practice for good information management, processing and handling. Turn2us recognises its obligations to those with whom it does business to process data reasonably and fairly.

This policy applies to information relating to identifiable people (i.e. Personal Data and Sensitive Personal Data). Its purpose is to enable Turn2us to:

- comply with the law in respect of the data it holds about people;
- follow good practice;
- protect its Individuals;
- protect itself.

Definitions of capitalised terms can be found in the annex. This policy should be read in conjunction with the IT Acceptable Usage Policy.

Policy Statement

Turn2us is a Data Controller as defined under the DPA. It may also act as a Data Processor when providing services to other organisations (see annex for definitions).

Turn2us will:

- not only comply with the law but also monitor good practice guidelines from main charitable umbrella bodies and follow these where appropriate;
- respect people's rights;
- be open and honest with those whose data is held;
- provide training and support for Individuals who handle personal data, so that they can act confidently and consistently;
- ensure that all partners with whom we work operate to the standards required by the DPA, and, if relevant, European data protection legislation.

Not causing harm to people is a priority for Turn2us. This means:

- keeping information securely in the right hands;
- holding good quality, accurate information;
- not holding information for longer than necessary.

Turn2us has a designated Data Protection Officer (DPO) to provide advice and guidance on matters related to data protection.

Issued: Jun 2005
Revised: Jan 2010, Jan 2011, August 2011 Sep 2016
Reviewed Nov 16 (typos only)

10.1 – Data Protection & Confidentiality

All Individuals are required to read, understand and accept any policies and procedures that relate to the personal data that Turn2us holds (e.g. this policy and any retention of data guidance).

Confidentiality often applies to a wider range of information than covered by data protection. In cases where someone will be working with confidential information they will be required to work within the remit of any departmental guidelines.

1. Guidance on Application of Policy

Staff should ensure they know who the current DPO is by consulting their line manager or HR.

This guidance of application of policy is not meant to be exhaustive, and should be read in conjunction with applicable law and any training given.

Security
In order to ensure that Turn2us is complying with the DPA, all Individuals who have responsibility for, or hold, personal data, either on a computer system or any other 'relevant filing system' (including paper) are responsible for its secure processing and storage. In effect, this means that the physical data shall be stored under lock and key when not in use and that suitable security systems are in place for electronic storage.

Principles of Good Information Handling
Individuals are required to ensure they are up to date with DPA training and comply with the DPA's eight principles of good information handling relating to Personal Data.

- 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/EFC's entry in the ICO 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 (therefore there is a need to regularly cleanse both electronic and paper records);
- 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.

10.1 – Data Protection & Confidentiality

Practical examples of good information handling might include:

- ensuring that all systems are accurate, up to date and processed in accordance with the DPA;
- only disclosing personal data where authorised, and then only in accordance with the DPA on a 'need and right to know' basis;
- treating all personal data with care;
- checking the identities of people before disclosing information by telephone, e-mail or letter;
- ensuring that their security measures are adequate (locks, passwords etc);
- not leaving computer screens unattended when 'logged in';
- keeping a 'clear desk' policy (disposing of waste printed matter as confidential waste);
- removal/redaction of non-essential personal data when storing or sharing information.

Sensitive Personal Data
The DPA makes specific provision for Sensitive Personal Data (see annex for definition). Sensitive personal data can only be processed under strict conditions including:

- having the explicit consent of the each and every 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.

Concerns or Failure to Comply
If a member of staff believes that there has been a failure to comply with DPA principles they must seek the guidance their line manager (who in turn must discuss with the DPO) or the DPO directly. No Individual should fear doing so – see the Whistleblowing Policy.

Right of Subject Access
The DPA allows Data Subjects to find out what information is held about themselves on computers and in some paper records. This is the Right of Subject Access. In addition the Data 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.

All Right of Subject Access requests must be passed to the DPO (or designate) within two working days. He/she will note the request and direct the process. The DPO has a duty to ensure the request is complied with within 40 days of request.

Third Party Requests
Request for information from outside bodies (such as the police, HMRC, journalists) should be immediately passed to the DPO (or designate) and the appropriate director/head of department.

Typically the DPO will consider the request in relation to the strict wording of the DPA. In the

case of the police and HMRC this will typically be in the form of a written request explaining the reason for the request. In the case of local authorities or government departments, the legal authority must be established. The Information Commissioner's Office may be consulted.

Training
Individuals' training in Data Protection is mandatory unless the member of staff is not involved in the processing of Personal Data or Sensitive Personal Data (see Annex for definitions). It is each Individual's responsibility to ensure they are up to date with policy using the materials provided and should ensure they review the training material at least annually.

The Freedom of Information Act 2000

Turn2us is not bound by the Freedom of Information Act. It does however uphold the spirit of the act in its broadest sense and believes that people have a right to know about its activities unless there is a compelling reason otherwise (such as vexatious requests, DPA compliance, competition etc.).

Information held about Employees

The DPA regulates the way in which certain information about Individuals is held and used. This section of the policy provides details about the type of information that Turn2us keeps about Individuals and the purposes for which it keeps this information.

Throughout the employment/relationship with Turn2us, and for as long a period as is necessary following the termination of employment/relationship, Turn2us will need to keep information for purposes connected with an Individual's employment, including recruitment and termination information. These records may include:

- information gathered about an Individual and any references obtained during recruitment or engagement.
- details of terms of employment/engagement.
- payroll, tax and national insurance information.
- performance information.
- details of grade and job duties.
- health records.
- absence records, including holiday records and self-certification forms.
- details of any disciplinary investigations and proceedings.
- training records.
- contact names and addresses.
- correspondence with Turn2us and other information provided to Turn2us.

Turn2us believes these uses are consistent with our employment/relationship and with the principles of the DPA. The information held will be for our management and administrative use only but, from time to time, we may need to disclose some information we hold about employees to relevant third parties e.g. where legally obliged to do so by HMRC or requested to do so by an Individual for the purposes of giving a reference. We may also

Issued: Jun 2005
Revised: Jan 2010, Jan 2011, August 2011 Sep 2016
Reviewed Nov 16 (typos only)

10.1 – Data Protection & Confidentiality

transfer information to another group or organisation, solely for purposes connected with an Individual's career or the management of Turn2us business.

It should also be noted that Turn2us might hold information about an Individual for which disclosure to any person will be made only when strictly necessary for the purposes set out below:

- an Individual's health, for the purposes of compliance with our health and safety and occupational health obligations.
- for the purposes of human resources management and administration e.g. to consider how an Individual's health affects their ability to do their job and, if the employee is disabled, whether they require any reasonable adjustment to be made to assist them in their role.
- the administration of payroll, insurance, pension, sick pay and any other related benefits in force from time to time.
- in connection with convictions to enable us to assess an employee's suitability for employment/engagement.

Employee Right of Access to Information
In accordance with the DPA all Individuals have the right to access any personal data that is being kept about them either on computer or in certain files.

An Individual who wishes to exercise this right should make this request in writing to the HR Department. Turn2us will aim to comply with any request for access to personal information without delay.

Turn2us may seek a payment of up to £10 to provide access to any personal data in accordance with regulations.

Turn2us requires all Individuals to comply with the DPA in relation to the information about other Individuals. Individuals in a position that deals with personal information about other Individuals must treat this information in strict confidence. Any deliberate breach of this Policy will be regarded as serious misconduct and will be dealt with in accordance with Turn2us Disciplinary Policy and Procedures.

Individuals Handling Personal Data

All Individuals have a duty, both during their employment/relationship with Turn2us and after their employment/relationship has ended, not to reveal any confidential information unless required to do so by a court of law.

Turn2us Contracts of Employment contain a confidentiality clause, which details Individuals' responsibilities.

If Individuals are asked for information which they think is or may be confidential, they must consider the following:

10.1 – Data Protection & Confidentiality

- All media (press, television, etc) enquiries must be referred in the first instance to the communications department at headquarters. It is important that no interviews or statements should be given without prior clearance.
- All enquiries from the police should be referred to the HR Department and/or the DPO as appropriate.
- Individuals required to give evidence in a court of law should inform the appropriate director/head of department or HR without delay.

Individuals requiring access to another Individual's email or personal files (e.g. after the Individual has left the organisation) must refer to IT and/or HR. Any access permitted will normally be supervised by IT and/or HR to help maintain confidentiality.

If in doubt staff should consult their line manager and/or the DPO.

Annex - Definitions

Data Controller	A person or organisation who determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Protection Act 1998 (DPA)	The UK legislation that provides a framework for responsible behaviour by those using personal information.
Data Protection Officer (DPO)	The person(s) responsible for ensuring that the organisation follows its data protection policy and complies with the Data Protection Act 1998
Data Processor	In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Subject	Means an individual who is the subject of personal data.
Information Commissioner's Office (ICO)	The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.
Personal data	Personal data means data which relate to a living individual who can be identified – (a) from those data, or (b) 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.
Right of Subject Access	The right of an individual who makes a written request (and pays a fee) to be told whether any personal data is being processed; given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; given a copy of the information comprising the data; and given details of the source of the data (where this is available) and the reasoning behind any automated decisions, such as a computer-generated decision. Responses to Subject Access requests must be prompt and within 40 days.
Sensitive personal data	Means data about racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, criminal record, criminal proceedings relating to a Data Subject's offences

//End

Issued: Jun 2005
Revised: Jan 2010, Jan 2011, August 2011 Sep 2016
Reviewed Nov 16 (typos only)