

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Purpose and Scope

This policy covers the charity Elizabeth Finn Care ('EFC'), trading as Turn2us. It applies to all Turn2us' trustees, employees, contractors, volunteers and other agents (hereafter collectively referred to for brevity as 'Team Members'). This policy has two main purposes:

- To detail Turn2us' expectations regarding the handling of personal and sensitive data relating to any individual (typically contacts, beneficiaries, customers etc).
- To explain the information Turn2us holds on Team Members.

Turn2us actively promotes compliance with, and broad awareness of, the General Data Protection Regulation ('GDPR', ratified 2016) 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 Special Categories of Personal Data as identified in GDPR). Its purpose is to enable Turn2us to:

- comply with the law;
- follow good practice;
- protect its Team Members;
- protect itself.

Definitions of capitalised terms can be found in Annex 1. This policy should be read in conjunction with the IT Acceptable Usage Policy.

Policy Statement

All Team Members 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 GDPR. For example, information that is confidential because of commercial interests, rather than personal rights. In cases where someone will be working with confidential information they will be additionally required to work within the remit of specific organisational or departmental guidelines or sign non-disclosure agreements etc. These guideline should include mechanisms for support, reporting and management of breaches etc.

Turn2us is a Data Controller as defined under the GDPR. It may also act as a Data Processor when providing services to other organisations.

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 it holds;
- provide training and support for Individuals who handle Personal Data, so that they can act confidently and consistently;

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

- gain assurance that all partners with whom we work operate to the standards required by the GDPR, and, if relevant, other 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;
- only holding information that is necessary and proportionate for the conduct of its business

Turn2us designates a Data Protection Officer (DPO) to provide advice and guidance on matters related to data protection. This person may be external to the organisation to reduce conflict of interest.

1. Guidance on Application of Policy

Team Members can find out who the current DPO is by consulting their manager or HR. However, because the DPO is likely to be external to Turn2us, any contact should be via or under the instruction of a member of the Senior Management Team (SMT) or HR. This is to avoid duplication of requests and effective use of existing guidance material.

Team Members are required to ensure they are up to date with GDPR training and comply with the GDPR's principles of good information handling (see below). These principles must also be considered in the design and implementation of all processes and procedures involving Personal Data.

This guidance on 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 GDPR, all Team Members who have responsibility for, or hold, Personal Data, either on a computer system or any other relevant system (including paper) are responsible for its secure processing and storage. In effect, this means that physical data shall be locked away when not in use and that suitable security systems are in place for electronic storage.

Principles of Good Information Handling

GDPR (Article 5) requires that Personal Data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals;
- b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- f. processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(taken from: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/>)

Practical examples of good information handling might include:

- ensuring that all systems are accurate, up to date and processed in accordance with the GDPR;
- only disclosing Personal Data where authorised, and then only in accordance with the GDPR 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 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.
- when appropriate ensuring Personal Data is pseudonymised (eg key-coded). It is important to consider how difficult it is to attribute the pseudonym to an individual.

Special Categories of Personal Data

The GDPR equivalent of the DPA's Sensitive Personal Data is 'Special Categories of Personal Data'. It includes information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics for ID, health, sex life and orientation. Unlike the DPA it does not include data relating to criminal offenses and convictions, because these are addressed by specific safeguards elsewhere in the GDPR).

Like Personal Data, you must still have a lawful basis for processing Special Categories of Personal Data, but because it is more sensitive it has more protection. To process it you need to satisfy a special condition (specified in Article 9 of the GDPR). The conditions of Article 9 are listed in Annex 2.

Children's Personal Data

The GDPR recognises that children need particular protection when their personal data is collected and processed because they may be less aware of the risks involved. The circumstances within which Turn2us processes children's data is usually via consent of parent/guardian; we would not normally process children's data directly from a minor. Since the

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

issues surrounding the protection of children and their personal data is complex, the DPO should always be consulted should there be new processes or changes to existing processes that involve children's data, Team Members should also refer to 'New and Changed Processes, Projects and Initiatives' below.

Concerns or Failure to Comply

If a Team Member believes that there has been a failure to comply with the GDPR, or is concerned about a practice that may potentially result in contravention of the GDPR, they must seek the guidance their line manager (who in turn must discuss with SMT, who potentially consult the DPO). Team Members who do not have a direct line manager (e.g. contractors and similar) should seek guidance from their main Turn2us contact or Head or relevant Department (who in turn must discuss with SMT, who potentially consult the DPO). Team Members should not contact external agencies such as the ICO directly; this should be done by SMT to ensure a coordinated overview of any situation is presented.

No Team Member should fear raising concerns – see the Whistleblowing Policy or equivalent for non-contracted Team Members.

Individuals rights

The GDPR provides the following rights for individuals (i.e. people who engage with Turn2us including Team Members):

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

The Office of Information Commissioner website (www.ico.org.uk) should be used as the primary source for guidance on these rights. However, this guidance provides and overview:

1. The right to be informed

This covers Turn2us' obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how Turn2us use Personal Data.

Any Team Member creating systems or processes should ensure that data protection/GDPR is an explicit part of the project plan and that the appropriate member of SMT is informed. It is then SMT's responsibility to ensure the system is reviewed by the DPO (they may designate this).

2. The right of access

Under GDPR, individuals have the right to obtain confirmation that their data is being processed; access to their Personal Data; and other supplementary information which largely corresponds to the information that should be provided in Turn2us' privacy notice.

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Turn2us requires that all Right of Access requests must be passed to SMT within one working day. Depending on the circumstances the DPO may be involved. Turn2us has a duty to ensure the request is complied with within one month of request.

Normally the request must be fulfilled free of charge. A fee based on the administrative cost can only be charged in cases where a request is manifestly unfounded or excessive (particularly if it is repetitive).

3. The right to rectification

Individuals are entitled to have Personal Data rectified if it is inaccurate or incomplete.

If Turn2us has disclosed the Personal Data in question to others, each recipient must be contacted and informed of the rectification - unless this proves impossible or involves disproportionate effort. If asked to, Turn2us must also inform the individuals about these recipients.

Turn2us must respond to the request within one month (this can be extended by two months where the request for rectification is complex). Where Turn2us is not taking action in response to a request for rectification, this must be explained, along with the individual's right to complain to the supervisory authority and to a judicial remedy.

4. The right to erasure

Also known as the 'right to be forgotten', this is complex and not an absolute right. In general terms, Personal Data must be erased when no longer necessary; if consent is withdrawn or if the processing is objected to or was unlawful. However, there are some specific circumstances where the right to erasure does not apply.

If, as a Team Member, you receive a request for erasure you must inform your manager or any member of SMT within one working day

6. The right to restrict processing

Such a request would mean that Turn2us is allowed to store the data, but not further process it. After such a request Turn2us would be able to retain just enough information to ensure the restriction is respected in future.

If, as a Team Member, you receive a request to restrict processing you must inform your manager or any member of SMT within one working day.

7. The right to object

Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (again including profiling) and processing for purposes of scientific/historical research and statistics.

The most likely of these reasons to affect Turn2us is that of direct marketing, though research and statistics is also possible. Turn2us must inform individuals of their right to object "at the point of first communication" and in its privacy notice. There must be a way to object online.

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

As a Team Member, you must inform your manager (or Turn2us point of contact if appropriate) of any such request, and whether you are able to comply. Managers should ensure that the request is complied with in accordance with the Individuals' Rights and Subject Access Request Policy .

8. Rights in relation to automated decision making and profiling

If a request is received from an Individual, team Members should manage this in the same way as other requests (above).

In addition, any Team Member creating systems or processes that involves automated decision making or profiling should insure that data protection/GDPR is an explicit part of the project plan and that the appropriate member of SMT is informed. It is then SMT's responsibility to ensure the system is reviewed by the DPO (they may designate this).

Third Party Requests

Request for information from outside bodies (such as the police, HMRC, journalists) should be immediately passed to the appropriate Director/Head of Department, or in their absence any member of SMT. Typically they will refer this to the DPO unless the request is straightforward.

The request will be considered in accordance with the strict wording of the GDPR. 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 DPO and/or the Information Commissioner's Office may be consulted.

Training

Team Member training in Data Protection is mandatory unless the Team Member is not involved in the processing of Personal Data. It is each Team Member's responsibility to ensure they are up to date with policy using the materials provided and should ensure they review relevant training material and/or training sessions at least annually, or as agreed departmentally with the DPO or authorised deputy.

New and Changed Processes, Projects and Initiatives

It is important that data protection and the GDPR are inherent in the design of any new processes, projects and initiatives and also formally considered as part of any changes to existing processes, projects and initiatives. Those managing the new or existing process, project or initiative must document the personal data implications and ensure they are assessed and approved by the DPO or authorised deputy. This assessment will include both the handling and storage of personal data. In many instances this will be covered by the Data Protection Impact Assessments of the project management methodology used.

It is recognised that for changes a degree of pragmatism is required – for example the DPO would not need to be consulted if a column title was changed from 'Surname' to 'Lastname'. If in doubt, guidance from a line manager should be sought.

The Freedom of Information Act 2000

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

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, GDPR compliance, competition etc.).

Information held about Team Members

The GDPR regulates the way in which certain information about Team Members is held and used. This section of the policy provides details about the type of information that Turn2us keeps about Team Members 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 a Team member's employment/relationship, including recruitment and termination/end of relationship information. These records may include:

- information gathered about a Team Member 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.
- 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 records are consistent with our employment/relationship and the principles of the GDPR. The information held will be for management and administrative use only but, from time to time, we may need to disclose certain information we hold about Team Members to relevant third parties e.g. where legally obliged to do so by HMRC, or requested to do so by a Team Members for the purposes of giving a reference. We may also transfer information to another group or organisation, solely for purposes connected with a Team Member's career or the management of Turn2us business.

It should also be noted that Turn2us might hold information about Team Members for which disclosure to another party will be made only when strictly necessary for the purposes set out below:

- a member of Team Member'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 a member of Team Member's health affects their ability to do their job and, if the

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Team Member 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 individual's suitability for employment/engagement.

Team Members Right of Access to Information

In accordance with the GDPR all Team members have the right to access any Personal Data that is kept about them either on computer or in certain files. Any Team Member who wishes to exercise this right should make this request in writing to the HR Department, or in the case of non-contracted Team Members, their manager or point of contact. Turn2us will aim to comply with any request for access to Personal Data without delay and within the timeframe required by the GDPR.

Turn2us would not normally make a charge for providing access to Personal Data. However, it reserves the right to charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive.

Turn2us requires all Team Members to comply with the GDPR in relation to the information about other Team Members. Team members in a position that deals with personal information about other Team Members must treat this information in strict confidence. Any deliberate or careless breach of this Policy will be regarded as serious misconduct and will be dealt with in accordance with Turn2us Disciplinary Policy and Procedures or equivalent policy and procedures for non-contracted Team Members.

Individuals Handling Personal Data

All Team Members 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 (or equivalent terms and conditions for non-contracted Team Members) contain a confidentiality clause, which details Team Members' responsibilities.

If a Team Members is asked for information which they think is or may be confidential, they must consider the following:

- 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 or a member of SMT (as appropriate).
- Team Members required to give evidence in a court of law should inform the appropriate Director/Head of Department or HR without delay.

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

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

If in doubt Team Members should consult their manager and/or HR. They in turn may consult the DPO.

Volunteers and other non-employed Team Members

Many aspects of this policy and guidance on its application refers to legislation and other policies and procedures that are only relevant to Turn2us employees. Therefore interpretation for volunteers and other non-employed Team Members should be amended accordingly in accordance with any related department policy/procedure.

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Annex 1 - 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.
GDPR	The General Data Protection Regulations as ratified by the European Union in 2016 and enforceable from 25 May 2018.
Information Commissioner's Office (ICO)	The UK Information Commissioner responsible for implementing and overseeing the GDPR.
Personal Data	Personal Data means data which relate to a living individual who can be identified – (a) from that data, or (b) from that 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 one month.
Sensitive Personal Data	A DPA definition that 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
SMT	Senior Management Team: the directors of the charity or authorised designates.
Special Categories of Personal Data	A GDPR category of data which is more sensitive than other Personal Data and specifically includes race, ethnic origin, politics, religion, trade union membership, genetics, biometrics for ID, health, sex life and orientation. Unlike the DPA Sensitive Personal Data it does not include data relating to criminal offenses and convictions, because these are addressed by specific safeguards elsewhere in the GDPR).
Team Member(s)	A collective term used in this document for Turn2us' trustees, employees, contractors and agents including voluntary agents.

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

Annex 2 - The conditions for processing special category data

The conditions are listed in Article 9(2) of the GDPR which are:

- (a) the data subject has given explicit consent to the processing of those Personal Data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the consent of the data subjects;
- (e) processing relates to Personal Data which are manifestly made public by the data subject;
- (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the Team Member, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Some of these conditions make reference to UK law, and the GDPR also gives member states the scope to add more conditions. Therefore this list may change over time and the above should not be considered exhaustive. The current regulations and legislation should be consulted.

TURN2US

Copies of all Turn2us HR Policies can be found on the Intranet. All Turn2us Team Members are subject to Turn2us HR Policies. Turn2us HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.1 – Data Protection & Confidentiality

DATA PROTECTION AND CONFIDENTIALITY POLICY AGREEMENT

I agree that will adhere to the terms of the Data Protection and Confidentiality Policy. Furthermore, I understand that serious violation of the policy may result in disciplinary and/or legal action being taken against me.

User's signature: _____

Print User's name: _____

Date: _____

Detach and return to the HR Department (or manager for non-employed Team Members).

//End