Data Protection Policy

Version Control

	Last Amended	Author	Action taken
0.1	20.8.18	Wayne Bullimore	Policy Created

Contents

Purpose

The purpose of this policy is to ensure that Reds in the Community and its staff (meaning permanent, fixed term, and temporary staff, any third party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with Reds in the Community), conduct their business practices in a manner compliant with the Data Protection Act 2018 ("DPA") and the General Data Protection Regulations (GDPR:2016) and its principles to ensure that all Personally Identifiable Information (PII) is secure, accurate and up-to-date at all times.

Scope

This policy applies to all members of the organisation and those contracted to work on behalf of Reds in the Community, and is to be followed at all times. Its aim is to protect the rights of individuals and applies to all personal and sensitive information that is used, stored and transmitted either electronically or via paper-based methods.

Objectives

The objective of this policy is to protect the rights of individuals with regards to the personal information known and held about them by Reds in the Community in the course of business and ensure that every business practice, task and process carried out by Reds in the Community, is compliant with each principle of the Data Protection Act 2018 and the General Data Protection Regulations (GDPR:2016)

Reds in the Community aim to ensure that staff are trained and aware of the guiding principles behind Data Protection of PII, namely to ensure;

- **Confidentiality** – That PII will be handled with due regard to its sensitivity and appropriate security measures put in place to maintain its confidentiality
- **Integrity** – That the PII which is held by Reds in the Community is up to date, accurate and can be relied upon.
- **Availability** – That the PII will be available to the data subject when they require the information.

This policy is therefore in place to ensure regulatory and legal compliance at all times with regards to handling and processing personal data.

Data Protection Policy Statement

Reds in the Community is classed as a Data Controller/Data Processor under the current Data Protection Act 2018, however Reds in the Community recognises that under the new General Data Protection Regulations (GDPR:2016) our obligations to ensure appropriate controls are in place irrespective of classification is of critical importance.

This policy confirms our commitment to protect the privacy of PII of our service users, clients, employees and other interested parties. Reds in the Community have engaged in a programme of Information Security Management which is aligned to the international standard, ISO 27001:2013 to ensure that the processes of personal information is conducted using best practice processes.

Basic Principles Regarding Personal Data Processing

The GDPR sets out a set of six guiding principles, which outline the responsibilities for organisations handling personal data. Article 5(2) of the GDPR states that *the controller shall be responsible for, and be able to demonstrate, compliance*. This is known as the 'Principle of Accountability'. The remaining policy statements demonstrate how Reds in the Community complies with these requirements.

(a) Lawfulness, Fairness and Transparency

Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals. Reds in the Community have taken steps to ensure that we understand the data that we control and/or process and have taken appropriate steps to establish the legal basis for this processing. Furthermore, we have taken steps to inform the data subjects what processing takes place and why.

(b) Purpose Limitation

Data shall be 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 is not considered to be incompatible with the initial purposes. Reds in the Community will only process data for the purpose it has been collected, and will not process data for other reasons without the consent or knowledge of the data subject(s)

(c) Data Minimisation

Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed and Reds in the Community have taken steps to ensure that data collected is not excessive and is appropriate to the purpose for which it is collected.

(d) Accuracy

Data shall be accurate and, where necessary, kept up to date; reasonable steps 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. Reds in the Community have established a process for reviewing and assessing accuracy of data and have processes in place to ensure any requests for rectification or erasure are addressed without undue delay.

(e) Storage Period Limitation

Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposed 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. Reds in the Community have established the retention periods of specific data sets, and will continually assess these to ensure they fit within appropriate legislation.

(f) Integrity and confidentiality

Data shall be 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 ('integrity and confidentiality'). Reds in the Community have established a robust Information Security culture within the organisation, which is continually managed and improved upon. This is in line with the international standard for information security, ISO 27001:2013.

Data Processing

Transmitting Personal Data

Where personal data is to be transmitted (either electronically or in hard copy), staff are required to ensure that any such data is secured using appropriate measures (e.g. Use of encryption, passwords for electronic transmissions or using secure couriers).

Personal Data will only be transmitted in accordance with best practice and processes noted as part of the ISMS.

Personal data is only transmitted to a person authorised to receive it in compliance with these Data Protection principles.

Storing Personal Data

Personal data in hard copies (e.g. paper medical records, copy passport etc) are retained only for as long as is essential to the account and/or customer, employee or other interested party that they refer to.

Personal data in hard copy or electronic formats will be stored in accordance with best practice and in line with processes, which are part of a broader Information Security Management System (ISMS).

The management of Personal Data is controlled through this standard and Reds in the Community have committed to ongoing audit and review of policies, processes and practices associated to holding information in all its form.

Breaches of Personal Data

If any breach of the DPA or its Principles occurs, staff are required to inform their line manager, who will report the details to the Compliance Officer to be logged and investigated, in line with Reds in the Community Incident Management processes.

Upon notification and initial investigation Reds in the Community will ensure that when deemed necessary, both the Information Commissioners Office and the data subjects affected will be informed without undue delay.

Roles & Responsibilities

This section outlines the key roles and responsibilities within Reds in the Community, involved in Information Security and Data Protection. These specific roles are assigned and communicated so that Information Security is not only managed effectively, but the performance of the security management system is reported through to the board of trustees.

It is critical for the functioning of the organisation that certain specific security roles and responsibilities be allocated to suitable individuals within the organisation.
The following roles must always be filled:

- Board of Trustees;
- Compliance Officer;
- Information Asset Owners.

There is however a general understanding throughout Reds in the Community that everyone has a role to play in Information Security. Therefore, each employee is equally responsible for his or her original task and for maintaining Information Security in the workplace at Reds in the Community .

Board of Trustees:

The board of trustees will always have overall responsibility for the suitability, adequacy and effectiveness of the ISMS within Reds in the Community In addition, and in line with the General Data Protection Regulation (GDPR), the board of trustees will be accountable for the protection of Personal Data, which is controlled or processed by Reds in the Community

In broad terms the responsibilities of the board of trustees are:

- To establish the ISMS policy, objectives and plans and ensure they are aligned with the strategic direction of the organisation;
- Ensuring the integration of the ISMS requirements into the organisations processes and communicating the importance of effective Information Security Management;
- Determine and provide appropriate resources to plan, implement, monitor and review information security and management;
- Directing and supporting the Compliance Officer to contribute to the effectiveness of the ISMS and conforming to the ISMS requirements;
- Ensuring the ISMS achieves its intended outcomes and promote continual improvement;
- Support the Senior Management Team to allow them to demonstrate their leadership as it applies to their areas of responsibility.

The board of trustees are responsible for the management of risk within Reds in the Community and ultimately responsible for acceptance of residual risks.

The Compliance Officer

The primary role of the Compliance Officer, in liaison with the board of trustees, is to ensure that the organisation processes the personal data of its staff, service users, partners or any other individuals in compliance with GDPR or the Data Protection Act 2018.

In broad terms the responsibilities of the Compliance Officer are:

- To communicate the importance and ensuring compliance of Information Security and the need for continual improvement across the organisation through the Senior Management Team;
- To conduct reviews of Information Security, at planned intervals;
- To serve as a point of contact between the organisation and the Information Commissioners Office (ICO);
- To deal with all 'subject access requests' in line with GDPR or the Data Protection Act 2018 requirements;
- To maintain a comprehensive record of all data processing activities conducted by the organisation, including the purpose of all processing activities which must be made public on request;
- To interface with data subjects to inform them about how their data is being used, their rights to have their personal data erased, and what measures the organisation has put in place to protect their personal information;
- To report any data breaches to the ICO in line with GDPR or the Data Protection Act 2018;
- To establish a continual improvement policy and culture across the organisation for Information Security;
- To discuss any projects which may impact upon the ISMS or on Data Protection;
- To review results of audits and exercises and address potential issues proactively;
- To identify, discuss and escalate risks within Reds in the Community
- To update the board of trustees on ISMS and Data Protection;
- To organise training and advice to relevant staff involved in ISMS and Data Protection.

Senior Management Team (SMT)

The role of the SMT is an important role, and has far reaching responsibilities and activities, to ensure the effective implementation of the ISMS. In summary the SMT is responsible for the following:

- Reporting to the Compliance Officer on all data security related matters on a regular basis;
- Helping foster an information security culture across the organisations workforce;
- Identifying and managing Data Protection risks associated with programme delivery;
- Communicating the Information Security Policy to all relevant personnel and service users as appropriate;
- Implement the requirements of the Information Security Policy and embed into programme delivery;
- Ensuring that no individual is given access to personal data without appropriate training and read relevant policy and guidance;
- Ensuring that internal processes and procedures are followed and are regularly reviewed;
- Ensure that security controls are documented (as appropriate) and implemented across service delivery;
- To ensure all areas of the Information Security Management System are reviewed at regular intervals and are imbedded into staff meetings;
- To ensure all staff are aware of their particularly responsibilities and they comply with information security and associated Data Protection processes and procedures; and
- To provide training and awareness briefings to staff on specific Information Security issues.

All employees

As stated previously, all employees of Reds in the Community receive appropriate training, where they are reminded of the role they have to play within Information Security, and the levels of responsibility they have.

Specific Roles

Facilities

Those responsible for the facilities used by Reds in the Community are responsible for physical security and suitably maintained to ensure a safe and secure environment.

Human Resources & Administrators

Administrators have an important role to play in ensuring the health and welfare of individuals within the organisation. In addition, they also have a role to play in ensuring that Personal Data is protected, and appropriate security in place to protect that information.

Technical and Organisational

The Data Protection Act states: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The organisation will implement the following measures to ensure compliance:

- Personnel files are confidential and are stored in locked filing cabinets;
- Only authorised employees have access to data;
- Files will not be removed from their normal place of storage without good reason;

- Personal data stored on discs, memory sticks, portable hard drives or removable storage media will be stored in locked filing cabinets or drawers when not in use by authorised employees.
- Personal data should not leave company premises without authorisation from the Compliance Officer;
- Data will be stored on computer shall be password protected, encrypted or coding and only authorised employees shall have access to that data;
- The organisation has network backup procedures to ensure that data stored electronically cannot be accidentally lost or destroyed;
- The implementation of forced password changes or password strength controls (all staff);
- The implementation of user/or group classification (Active Directory groups);
- Permission based file/folder staff access; and
- Segregated vLan network or Wi-Fi SSID's

Technical support and advice will be drawn from external agencies to ensure ongoing compliance.

The Rights of Access by Data Subjects

Section 3 of the GDPR states that data subjects have rights in relation to their data, including; Individuals under the GDPR have:

The right to be informed

Individuals have the right to be informed about how we use their personal data.
This includes:

- Who we are
- Any legal reason for us requiring their data
- How long we will keep their data for
- The existence of your rights under the General Data Protection Regulations

The right of access

Individuals have the right to obtain:

- Confirmation that their data is being processed by us
- Access to the personal data we hold on them (through the 'Subject Access Review' process)

The right to rectification

Individuals have the right to have their personal data rectified if it is inaccurate or incomplete

The right to erasure (the right to be forgotten)

Individuals have the right to request the deletion or removal of their personal data, where there is no compelling reason for its continued processing, such as at the end of their contract

The right to restrict processing

Individuals have the right to request that we restrict further processing of their personal data where:

- They contest the accuracy of the personal data we hold on them, until it has been rectified and verified
- They have objected to us processing their personal data (where there is a legitimate reason for the processing such as a performance of a contract) until their objection has been fully considered and a decision made
- Processing is unlawful and they request the process of their data be restricted instead of erased

The right to object

Where we process individual's personal data for the performance of their contract, they have the right to object to the processing however, this must be on grounds relating to their particular situation. In these circumstances, we will stop processing their personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, or
- The processing is for the establishment, exercise or defence of legal claims.

Where we process individuals personal data for direct marketing purposes, they have the right to object at any time.

If they object to their personal data being processed for direct marketing purposes:

- We will stop the processing as soon as we received their objection
- We will deal with their objection at any time and free of charge

Rights in relation to automated decision making and profiling

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, and
- It produces a legal effect or a similarly significant effect on them

We will **not** use individuals' personal information for any automated decision-making or profiling purposes.

When acting as a data controller, Reds in the Community is responsible for providing data subjects with a reasonable access mechanism to enable them to exercise these rights.

Legal Basis for Processing (Consent)

Article 6: Lawfulness of processing

Article 6 of the GDPR provides the legal basis under which personal data can be processed, and Reds in the Community uses the following, legal basis:

- ***Employee Data*** - Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

- ***Marketing and Promotional Material*** – The 'Legitimate Interests' of individuals will be considered for marketing purposes, and only where clear Consent has been obtained or where previous indications of interest have been shown.

Under these conditions, Reds in the Community will apply the following legal basis for processing personal data:

- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.

In all other circumstances, Reds in the Community apply the following legal basis for processing personal data:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Where consent is obtained from individuals directly

The GDPR states:

Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.

Silence, pre-ticked boxes or inactivity should not therefore constitute consent.

Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Where required, Reds in the Community obtains consent from individuals at the Registration Stage, via appropriate means. This is gained through the individual ticking a box, or signing a 'Consent form' and making a conscious decision to 'opt in'.

Subject Access Requests

Under Article 15 of the GDPR, an individual has 'The Right to Access' personal information which is being held about them by Reds in the Community. This information is to provided free of charge and individuals have the right to obtain:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;

Although the information will be provided free of charge, where there is an excessive request for data, or repetitive requests a 'reasonable fee' can be charged.

Any fee charged must be based on the administrative cost of providing the information and information must be provided without delay and at the latest within one month of receipt.

We are able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

It is important that we verify the identity of the person making the request, using 'reasonable means'. If the request is made electronically, we will provide the information in a commonly used electronic format (e.g. CSV, or PDF).

Definitions

To ensure Reds in the Community understands its obligations to the protection of Personal Information, the following definitions apply and are based on current understanding of these terms within UK and European law, and specifically in Article 4 of the GDPR.

Personal Data

Any information relating to an identified or identifiable natural person ("Data Subject") who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Personal Data

Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller

The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor

A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing

An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

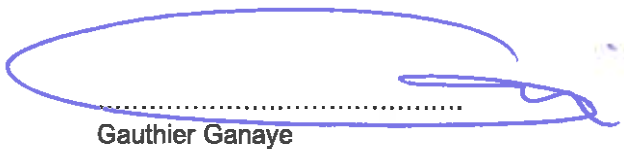
Anonymization

Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

This Policy

This policy is reviewed annually as part of the ongoing Information Security Management System (ISMS) process by the Reds in the Community.

Approved by the Board of Trustees on the 27.9.18 and was duly signed on its behalf by:



.....
Gauthier Ganaye