RESPOND
Support
Care, Education, Family, Community

Data Protection Policy & GDPR

Author:	Albert Perris
Contact	Respond Support Johns College, The Folly, Co Waterford. T: 01 8832 551 E: info@respondsupport.ie

Date Issued:	June 2018
Version	V2

1. Table of Contents

Document Change Log

Version	Date	Changed By	Description
1.0	April 18th 2018	Albert Perris	First draft
2.0	12th June 2018	Bonnie O' Sullivan	Final Draft

1. Document Objective

The purpose of this policy document is to:

- Set out Respond Support requirements under the Data Protection Acts, 1988 & 2003, GDPR 2018 and all other relevant regulations and Code of Practices
- Demonstrate our commitment to protect the rights and privacy of individuals in accordance with the Data Protection Acts
- Proactively ensure we meet our obligations in a transparent, ethical and consistent manner
- Set out the required standards for safe and effective record keeping
- Provide a robust data protection system by assessing, managing and auditing risks
- Provide a framework that preserves an individual's right of privacy and the Company's informational necessity to perform its duties

Scope and Responsibilities

This policy applies to all employees and/or agents of Respond Support who process personal data of individuals such as, but not limited to, our potential, current and former clients, service users, employees, volunteers, students, funders, partner companies, or any other person(s) or entities closely linked to the activities of the Company.

What is Data Protection?

Data protection is about creating a framework for the lawful processing and protection of personal data. It is the means by which an individual's fundamental right to privacy is safeguarded.

The Data Protection Acts, 1988 and 2003 confers specific rights on individuals as well as placing responsibilities on those persons processing personal data.

Definitions

The following definitions are used throughout this policy document:

Data means information in a form which can be processed. It includes both automated data and manual data.

Automated data means any data on a computer or data recorded with the intention of putting it on a computer.

Manual data means data that is kept as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

Relevant filing system means any set of data that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals, so that specific data is accessible.

Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Processing means performing any operation or set of operations on data, including:

- obtaining, recording or keeping data
- collecting, organising, storing, altering or adapting the data
- retrieving, consulting or using the data
- disclosing the data by transmitting, disseminating or otherwise making it available
- aligning, combining, blocking, erasing or destroying the data

Data Subject is an individual who is the subject of personal data.

Data Disclosure is the provision of personal data to a third party by any means whether written, verbally or electronically.

Data Controllers are those who, either alone or with others, control the contents and use of personal data.

Data Processor is a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his/her employment.

Sensitive Personal data is specific categories of data which are defined as data relating to either:

- the racial or ethnic origin, the political opinions or the religious or other beliefs of the data subject
- trade union membership of the data subject
- the physical or mental health or sexual life of the data subject
- criminal convictions or the alleged commission of an offence by the data subject

Data Collection

Data is essential to the effective delivery of Respond Support services. We hold data for a variety of purposes, which largely relates to the provision of care and support services and in the context of the administration of the Company.

Some examples of where the Company may collect, handle, manage, store and/or process data include but is not limited to:

- Performing accounting and other record-keeping functions
- Providing HR, payroll, pension and Death in Service (DIS) administration services
- Providing volunteer administration
- Monitoring and improving our service delivery by undertaking Client surveys or research
- Delivery of care supports and mental health services
- Delivery of childcare services and community-based initiatives
- Undertaking criminal record vetting checks in particular for Employees and Volunteers
- Providing general information, updates, public relations and advocacy of Company activities
- Complying with our legal, regulatory, funding and contractual obligations and in particular our obligations under statutory funding schemes through which our services are financed
- Planning for the future delivery of services to meet the on-going needs of our clients

Data Protection Principles

Respond Support shall perform our responsibilities under the Data Protection Acts in accordance with the following eight guiding principles:

- Obtain and process data fairly
- Keep data only for one or more specified, explicit and lawful purposes
- Use and disclose data only in ways compatible with these purposes
- Keep data safe and secure
- Keep data accurate, complete and up-to-date
- Ensure that data is adequate, relevant and not excessive
- Retain data for no longer than is necessary for the purpose or purposes
- Give a copy of his/her personal data to that data subject on request in a timely manner

We shall now examine each of these in more detail and outline a code of practical steps to protect data.

Obtain and Process Data Fairly

We shall obtain and process personal data fairly and in accordance with statutory and other legal obligations. In particular, the data subject will, at the time the personal data is being collected, be made aware of:

- the name of the data controller i.e. the Company
- the purpose for collecting the data
- the persons or categories of persons to whom the data may be disclosed, if any
- whether replies to any questions are obligatory and the consequences of not replying to those questions
- the existence of the right to access personal data
- the right to rectify data if inaccurate or processed unfairly
- any other information which is necessary so that processing may be fair and to ensure the data subject has all the information that is necessary so as to be aware as to how their data will be processed

In addition, where the personal data is not obtained from the data subject, either at the time their data is first processed or at the time of disclosure to a third party, all the above information will be provided to the data subject and they will also be informed of the identity of the original data controller from whom the data was obtained and the categories of data concerned.

Keep Data Only for One or More Specified, Explicit & Lawful Purposes

We shall keep data for a purpose(s) that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with that purpose(s). A data subject has the right to question the purpose for which we hold his/her data and must also be able to identify that purpose.

To comply with this rule:

- A data subject shall know the reason(s) why we are collecting and retaining their data
- The purpose for which the data is being collected shall be lawful
- We will be aware of the different sets of data that are kept and the specific purpose of each

Use and Disclose Data Only in Ways Compatible with These Purposes

We shall use and disclose personal data only in circumstances that are necessary for the purpose(s) for which we collect and keep the data. However, disclosures may be made by the Company where:

- an explicit consent has been received from the data subject
- it represents a vital interest of the data subject
- it is a requirement of law
- it is made to the data subject themselves
- it is necessary to meet a legal obligation or contractual necessity of the Company
- Child protection or vulnerable adult protection purposes
- Circumstance in which mandatory reporting procedures apply

In making a data disclosure, we shall consider whether the data subject would be surprised to learn that a particular disclosure is taking place. If the potential answer to this is yes, then there is a need to question the basis for the disclosure prior to making it.

In all cases the identity of the recipient of the disclosure should be established along with the specific purpose of the disclosure and the legal basis/power to disclose the relevant data. A record of all disclosures shall be maintained.

In particular, photographs or recording of any individual will only be published on Company material, advertisements and/or publications with the prior authorisation of the data subject.

Keep Data Safe and Secure

We shall take appropriate and all reasonable security measures against the unauthorised access to, alteration, disclosure or destruction of personal data and against its accidental loss or destruction. The nature of security used will take into account what technology is available, the cost of implementation and the sensitivity of the data in question.

A standard of security may include:

- Access to personal data shall be restricted to authorised staff on a strictly need-to-know basis
- Respond Support premises will be appropriately secured such as the use of locks, fobs etc.
- Access to the company's computer systems shall be password protected.
- Company mobile phones shall be protected with a pin number
- Passwords shall not be written down or shared with any other person
- All Company laptops will be encrypted
- Company computers shall not be left unattended and all computerised systems will be logged off and computers locked each time an employee leaves their workstation
- All entries on computer systems will be uniquely identifiable to the entering employee
- Appropriate measures shall be taken to ensure data is protected on Company systems such as anti-virus and firewall software

- Data on computer screens and manual files shall be kept hidden from callers to our offices
- Company laptops, portable electronic devices and/or paper files containing personal data shall not be left unattended in Employee cars. If they must be left un-attended they must be securely locked in the boot of the car.
- Where an Employee removes a paper file from Company offices to attend meetings, home visits, etc. the file will be keep in a suitable secure brief case
- The Company shall operate a clean desk policy where all files and documents will be secured while employees are not at their workstation.
- The downloading of data from Company computer systems to USB, CD or other devices or sent outside the Company via email or other means is strictly not permitted without the express written permission of the Company.
- Appropriate back-up procedures shall be in operation for computer held data
- All waste papers, printouts, etc. shall be disposed of carefully by shredding
- Paper based files shall be securely locked in damp-proof and fire-proof filing systems with keys only held by relevant persons
- Paper based files shall be kept intact with no parts or pages removed
- Where the Company engages a third-party Company to provide a service, sufficient written guarantees will be obtained from the service provider of data protection compliance
- All reasonable measures shall be taken to ensure that our staff are made aware of these security measures and comply with them

Keep Data Accurate, Complete & Up-to-date

We shall adopt appropriate procedures to ensure the highest levels of data accuracy, completeness and ensure that personal data is, at all times, up-to-date.

It should be remembered that personal data particularly in relation to client care can be required as evidence before a court of law. Data accuracy is therefore of the upmost importance.

The following shall also be noted:

- Records must be objective, factual and describe what is observed. If an incident has not been observed, but is relevant, then it must be clearly stated that it was not observed. If for some reason a more subjective statement needs to be made, the statement shall be acknowledged as a subjective opinion.
- Records shall not include jargon, subjective statements or abbreviations (other than those approved). All records will be written in a way that can be easily understood.
- All hand-written records shall be written legibly and indelibly. Records shall be clear, unambiguous and accurate including the date of entry and the printed name and signature of the person completing the record.
- Alterations to written records shall be made by scoring out the original data with a single line followed by the initialed and dated correct entry. The use of correction fluid such as 'Tipp-ex' is not permitted.

It shall be noted that the accuracy requirement does not apply to back-up data, that is, data kept only for the specific and limited purpose of replacing other data in the event of data being lost, destroyed or damaged.

Ensure that Data is Adequate, Relevant & Not Excessive

We shall only request and retain personal data that is adequate, relevant and not excessive. We shall fulfil this by ensuring we seek and retain only the minimum amount of personal data which we need to achieve our purpose(s).

Specific criteria will be used for each data need to assess what data is needed and not excessive. Periodic reviews will also be carried out on the relevance of personal data sought from data subjects in addition to reviews on the basis of any personal data already held.

Retain Data for No Longer than is Necessary

For the purposes of retention, data will be categorised into various data sets. The Company shall clearly define the length of time each data set will be kept based on objective and reasonable reasons. Data will be regularly purged and subject to the periods set out below in section 17, data will not be retained once the purpose for which it was collected has ceased.

Subject Access Requests

On making an access request any individual about whom we keep personal data is entitled to:

- a copy of the data we are keeping about the data subject
- know the categories of data and the purpose(s) for processing it
- know the identity of those to whom we disclose the data, if any
- know the source of the data
- know the logic involved in automated decisions
- data held in the form of opinions.

To make a subject access request the individual must:

- Download a *Subject Access Request Form* from www.respondsupport.ie or phone 01-8832 551 to request a form.
- Complete, sign and return the *Subject Access Request Form and return to the Data Co-Ordinator at Johns College, The Folly, Waterford X91 VO90.*
- Attach photocopy proof of identity such as a current driving license, passport or Public Services Card

In response to an access request the Company will:

- Acknowledge and reply to your request in writing within 10 working days, requesting if necessary, clarification or further information required by us to process your request in a timely manner.
- Collate the data, removing and/or retracting all data relating to any other persons
- Supply a copy of data, by registered mail, to the data subject within 20 working days of receiving the original written request, or of receiving the required clarification or further information as requested above
- Provide the data in a form that will be clear, for example, any codes will be explained

Subject access requests will only be disclosed in writing to the data subject concerned. Data will not be provided by phone. Subject access requests will only be disclosed to someone acting on the data subject 's behalf such as a solicitor upon receipt of confirmed written consent of the data subject.

Where we do not keep any data about the individual making the access request, we will duly inform the individual in writing, within 20 working days of receiving the original written request, or of receiving the required clarification or further information as requested above.

Subject Access Request Exclusions

The Company shall in limited and exceptional situations refuse and/or restrict a data subject's right of access such as but not limited to:

- If health or social work data would be likely to cause serious harm to the physical or mental health or emotional condition of the data subject (in accordance with the Data Protection (Access Modification) (Health) Regulations, 1989 and Data Protection (Access Modification) (Social Work) Regulations, 1989
- Where the circumstances are such that a claim of privilege could be maintained in court proceedings in relation to communications between the Company and our professional legal advisers or between those advisers
- If the data concerns an estimate of damages or compensation in respect of a claim against the Company, where granting the right of access would be likely to harm the interests of the Company
- Where it would prejudice the investigation of a criminal offence
- Where the supply of a permanent form copy is not possible or would involve disproportionate effort
- If the Company has already complied with an access request the Company does not have to comply with an identical or similar request unless a reasonable interval has elapsed

In any such event, the Company will write to the data subject within 20 working days outlining the reason(s) for such a refusal.

Sensitive Personal Data

Sensitive personal data may be held by the Company, only where necessary. It may also be held for employment purposes, for example, criminal record vetting of employees. Except in the narrow

exceptional circumstances set out in the Data Protection Acts, explicit consent will be obtained from the Data Subject in line with the Data Protection Acts in order to process such sensitive data.

Data Retention & Destruction

The table below sets out Respond Supports defined policy on retention periods for specific items of personal data:

Type of Record	Duration
Accident books, reports & records of accidents or dangerous occurrences	**7 years from date of entry**
Accounting & financial records & books, such as invoices, credit/debit notes, receipts, accounts, bank statements, etc.	**7 years after the financial year to which they relate**
Childcare files	**2 years after child has left the service**
Client case histories, therapeutic & care plans & key working notes	**7 years after the client has left the service**
Data disposal schedules	**Indefinitely**
Employee HR files	**7 years after employment ceases**
Employee pension records	**12 years after benefits cease**
Employee tax payment records	**7 years after the tax year to which they relate**
Employee working time and leave	**3 years after the leave year to which they**
Formal company documents such as statutory books, Board minutes & resolutions	**Indefinitely**
Records of all transactions that affect or may affect, the company's VAT liabilities	**7 years after the financial year to which they relate**
Recruitment campaign records and job interview/selection notes (for unsuccessful candidates)	**1 year (or longer if there is threat of legal action)**
Tender documentation from unsuccessful suppliers	**12 months**
Volunteer files	**7 years after volunteering ceases**

Where there is uncertainty on the retention period for any specific piece of data, it is good practice to keep records for six years plus one year to cover the general statute of limitation for civil legal action.

After the above periods, data will be confidentially shredded, destroyed and/or permanently deleted. On destruction of any data, a record of its destruction may be kept in a Disposal Schedule.

Correction of Data & Data Protection Complaints

If a data subject disagrees with data held about them the following shall be followed:

- If there is agreement about the changes, the data will be duly corrected.
- If there is disagreement about the changes then this will be noted on the file and the matter referred to the Data Protection Coordinator for review.

Data Protection complaints shall, in the first instance, be addressed to the Data Protection Coordinator. Data Protection complaints from a Company employee shall be directed through the Company's Grievance or Whistleblowing procedures.

Policy Updates & Enforcement

This document shall be considered a Respond Support policy document and is made under and shall be construed and interpreted in accordance with the laws of the Republic of Ireland. This policy is written to reflect current custom, practice and legislative environment and will be reviewed, updated and ratified as necessary.

All employees and agents of the Company who collect, control, process and/or use personal data are individually responsible for compliance with this policy. The Company's Data Protection coordinator shall ensure the provision of support, assistances, advice and training throughout Respond Support. The Company's Senior Management Team shall ensure compliance with the Data Protection Acts and GDPR

Data Protection Audits

To ensure the quality of data retained by the Company and that access to and usage of such data is appropriate within the terms of this policy document, each Manager within the Company as part of his/her duties shall regularly audit and examine data under the headings of quality control, data accuracy, access to and security of data and usage of data.

In addition to this, the Data Protection Coordinator will conduct examinations and reviews of Data Protection procedures as part of their ongoing examination and review process.

Furthermore, external audits of all aspects of Data Protection within the Company may be conducted on a periodic basis.

Further Details

All data protection queries should be directed to:

Data Protection Coordinator
Respond Support
Johns College,
The Folly,
Co Waterford.
T: 01 8832 551
E: info@respondsupport.ie