Policy	S:\Policy and Procedures
Data Protection & Privacy [GDPR] Policy	Issue: 3
	Date: September 2019
	Approver: Rob Williams

1 Purpose and Scope

This policy provides

- a framework for ensuring that Connection Support meets its obligations under the General Data Protection Regulation (GDPR) and associated legislation[1] ('data privacy legislation') and supports the 7 Caldicott Principles.
- Procedures for data protection by design and by default

This policy applies to all processing of personal data carried out for the Charity's purpose, irrespective of whether the data is processed on non-charity equipment or by third parties.

> **'*Personal data*'** means any information relating to an identifiable living individual who can be identified from that data or from that data and other data. '*Processing*' means anything that is done with personal data, including collection, storage, use, disclosure and deletion.

More stringent conditions apply to the processing of special category personal data.

> **'*Special category*'** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

> '***Processing***' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes paper based and electronic personal data.

This policy should be read in conjunction with the accompanying guidance, and supporting policies and procedures which provides further detail and advice on practical application, as well as any

other documents that impose confidentiality or data management obligations in respect of information held by Connection Support.

This policy does not cover the use of personal data by members of Connection Support when acting in a private or non-company capacity.

[1]This includes all legislation enacted in the UK in respect of the protection of personal data as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003.

2 Background

The processing of personal data underpins almost everything Connection Support does. Without it, clients cannot be supported; staff cannot be recruited; and events cannot be organised for visitors.

We are responsible for handling people's most personal information. By not handling personal data properly, we could put individuals at risk.

There are also legal, financial and reputational risks for Connection Support. For example:

- If we are not able to demonstrate that we have robust systems and processes in place to ensure we use personal data properly we might lose our ability to carry out support services requiring access to personal data, particularly in the services to our clients.
- Reputational damage from a breach may affect public confidence in our ability to handle personal information.

The Information Commissioners Office (ICO), which enforces data privacy legislation, has the power to fine organisations up to 4% of global annual turnover for serious breaches.

3 Principles

We acknowledge our accountability in ensuring that personal data shall be:

- processed fairly, lawfully and in a transparent manner;
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, up-to-date;
- not kept for longer than necessary; and
- kept safe and secure.

In addition, a new accountability principle requires us to be able to evidence compliance with these principles.

We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies taking into account all relevant legislation and individual consent.

Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in Privacy Notice . We ensure that it is as easy to withdraw as to give consent.

4 Aims and Commitments

Connection Support handles a large amount of personal data and takes seriously its responsibilities under data privacy legislation. It recognises that the mishandling of an individual's personal data may cause them distress or put them at risk of identity fraud. As a result, it is committed to:

- complying fully with data privacy legislation;
- where practicable, adhering to good practice, as issued by the ICO or other appropriate bodies; and
- handling an individual's personal data in a careful and considerate manner that recognises the importance of such information to their privacy and welfare.
- Undertaking annual audits of our compliance

Connection Support seeks to achieve these aims by:

- ensuring that staff, volunteers and other individuals who process data for Connection Support purposes are made aware of their individual responsibilities under data privacy legislation and how these apply to their areas of work. For example, employment contracts include a clause drawing the attention of the employee to data privacy legislation and Connection Support's data protection policy;
- providing suitable training, guidance and advice. Connection Support's online training course on data privacy and information security is available to all members of Connection Support. The online course is supplemented by bespoke on-site training, where appropriate, along with regular talks and presentations at departmental meetings.
- incorporating data privacy requirements into administrative procedures where these involve the processing of personal data, particularly in relation to major information systems (the concept of 'privacy by design');
- operating a centrally coordinated procedure (in order to ensure consistency) for the processing of subject access and other rights based requests made by individuals; and

investigating promptly any suspected breach of data privacy legislation; reporting it, where necessary, to the ICO; and seeking to learn any lessons from the incident in order to reduce the risk of reoccurrence

5. Data Protection by Design and Default

We shall implement appropriate organisational and technical measures to uphold the principles outlined above.

- We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.
- We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.
- Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA)
- All new systems used for data processing will have data protection built in from the beginning of the system change.
- All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.
- We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.
- In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.
- Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

6. Data Security

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

The following measures will be taken as a minimum:

- Using lockable cupboards (with restricted access to keys)
- Password protection on personal information files
- Computer systems that allow restricted access to certain areas
- Not allowing personal data to be taken off site (as hard copy, on laptop or on memory stick)
- Back up of data on computers (onto a separate hard drive / onto tapes kept off site)

- Password protected attachments for sensitive personal information sent by email
- Use of Egress / encryption software as required for different contracts

The Board and trustees are accountable for compliance of this policy.

7. Data Quality

Good quality, accurate records are vital for the safety of our service users and the safe and responsible running of our organisation.
We will ensure that all personal data stored has the following characteristics: -

a) It is *authentic* – i.e. the data is what is claims to be.

b) It is *reliable*.

c) It has *integrity*.

d) It is *useable*. – ie we can find it

6. Roles and Responsibilities

Board member

Board member has executive responsibility for ensuring that Connection Support complies with data privacy legislation.

It is supported by its ***Board member*** *Committee*, which is responsible for keeping under review Connection Support's policies and compliance with legislation and regulatory requirements.

Data Protection Officer (DPO)

The DPO is responsible for monitoring internal compliance, advising on Connection Support's data protection obligations and acting as a point of contact for individuals and the ICO.

Information Compliance Officer/Data Protection Officer

The Information Compliance Officer is responsible for:

- establishing and maintaining policies and procedures at a central level to facilitate Connection Support's compliance with data privacy legislation;
- establishing and maintaining guidance and training materials on data privacy legislation and specific compliance issues;
- supporting privacy by design and privacy impact assessments;
- responding to requests for advice from departments/operations;

- coordinating a Connection Support's -wide register exercise to capture the full range of processing that is carried out;
- complying with subject access and other rights based requests made by individuals for copies of their personal data;
- investigating and responding to complaints regarding data privacy (including requests to cease the processing of personal data); and
- keeping records of personal data breaches, notifying the ICO of any significant breaches and responding to any requests that it may make for further information.

In fulfilling these responsibilities, the team may also involve, and draw on support from, representatives from other departments and operations.

Senior Managers

Senior Managers are responsible for ensuring that the processing of personal data in their department conforms to the requirements of data privacy legislation and this policy. In particular, they must ensure that:

- new and existing staff, visitors or third parties associated with the department who are likely to process personal data are aware of their responsibilities under data privacy legislation. This includes drawing the attention of staff to the requirements of this policy, ensuring that staff who have responsibility for handling personal data are provided with adequate training and, where appropriate, ensuring that job descriptions for members of staff or agreements with relevant third parties reference data privacy responsibilities.
- adequate records of processing activities are kept (for example, by undertaking register exercises);
- data protection requirements are embedded into systems and processes by adopting a 'privacy by design' approach and undertaking privacy impact assessments where appropriate;
- privacy notices are provided where data is collected directly from individuals or where data is used in non-standard ways;
- data sharing is conducted in accordance with Connection Support's guidance;
- requests from the Information Compliance Officer for information are complied with promptly;
- data privacy risks are included in the department's risk management framework and considered by senior management on a regular basis; and
- departmental policies and procedures are adopted where appropriate.
- that all buildings used by the organisation have suitable security measures and that staff are provided with the appropriate equipment to keep personal data safe.

Staff, Contractors, volunteers and third parties

Anyone who processes personal data for the Company's purpose is individually responsible for complying with data privacy legislation, this policy and any other policy, guidance, procedures, and/or training introduced by Connection Support to comply with data privacy legislation.

They must ensure that they:

- Understand and act in line with this policy and all related guidance
- only use personal data in ways people would expect and for the purposes for which it was collected;
- use a minimum amount of personal data and only hold it for as long as is strictly necessary;
- keep personal data up-to-date;
- keep personal data secure, in accordance with Connection Support's Information Security Policy;
- do not disclose personal data to unauthorised persons, whether inside or outside Connection Support;
- complete relevant training as required;
- report promptly any suspected breaches of data privacy legislation, in accordance with the procedure in section 6 below, and following any recommended next steps;
- seek advice from their line manager or Information Compliance Officer where they are unsure how to comply with data privacy legislation; and
- promptly respond to any requests from the Information Compliance Officer in connection with subject access and other rights based requests and complaints (and forward any such requests that are received directly to the Information Compliance Officer promptly).

Third party processors will sign Sub Processor agreements and be required to provide proof of their organisational GDPR compliance.

8. Breaches of data privacy legislation

Connection Support will investigate incidents involving a possible breach of data privacy legislation in line with our Data Breach Procedure, in order to ensure that, where necessary, appropriate action is taken to mitigate the consequences and prevent a repetition of similar incidents in future. Depending on the nature and severity of the incident, it may also be necessary to notify the individuals affected and/or the ICO. A breach will occur where, for example, personal data is disclosed or made available to unauthorised persons or personal data is used in a way that the individual does not expect.

Incidents involving failures of IT systems or processes must be reported to the Bluespires within 4 working hours of discovery. Bluespires will liaise, as appropriate, with the Information Compliance Officer and Data Protection Officer.

Where Connection Support's role is as Data Processor as determined by contractual relationship, notifications of potential breaches will be made to the Data Controller as per contract.

Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary proceedings.

Any unauthorised disclosure of personal data to a third party made by a volunteer may result in the termination of the volunteering agreement.

Any unauthorised disclosure of personal data to a third party made by a Trustee could result in a penalty arising from a breach that they have made which they would be personally liable for

All other incidents must be reported directly to the Information Compliance Officer at the earliest possible opportunity.

9. Subject Access Request

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to: dpo@connectionsupport.org.uk or, Data Protection Officer, Connection Support, 213 Barns Road, Cowley, Oxford, OX4 3UT

We may make a charge of £10 on each occasion access is requested.

The following information will be required before access is granted:

- Full name and contact details of the person making the request
- their relationship with the organisation (former/ current member of staff, trustee or other volunteer, service user
- Any other relevant information- e.g. timescales involved

We may also require proof of identity before access is granted such as Full UK Driving Licence, Passport, Birth Certificate

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request and relevant fee.

9. Compliance

Connection Support regards any breach of data privacy legislation, this policy or any other policy and/or training introduced by Connection Support from time to time to comply with data privacy legislation as a serious matter, which may result in disciplinary action. Depending on the nature of the breach, an individual may also find that they are personally liable (for example, it can be a criminal offence for a member of Connection Support to disclose personal information unlawfully).

The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner's Office (ICO). We notify and renew our notification on an annual basis as the law requires.

If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is Rob Williams..

10. Further information

Questions about information security, this policy and data privacy matters in general should be directed to the Business Systems and Facilities manager, who can be contacted on dpo@connectionsupport.org.uk.

11. Review and development

This policy will be reviewed at intervals of 1 year to ensure it remains up to date and compliant with the law.

12. Related policies

This policy is underpinned by::

- Information Security and Data Sharing Policy
- Regulations relating to the use of Information Technology Facilities.
- Guidance – Data Protection in Practice
- Data Breach Notification Policy

- Information Classification Policy

13. Document Contributors

Principal author(s): Joanne Simpkins, Human Resources Manager

Contributor(s): Alice Copping, Operations and Development Manager

14. Document Changes

Monitoring: This procedure will be reviewed periodically to ensure compliance with changes in employment law and equality and diversity legislation.

Issue No.	Date	Changes	Changes made by/ authorised person
1	25 May 2018	First issue.	
2	10 January 2019	Reviewed	
3	3 September 2019	Updated to include info on SAR, data security, breaches, Design and default	Alice Copping
4	28 May 2020	Updated name of DPO registered with ICO	Alice Copping

STAFF DECLARATION

I confirm I have read and understood Connection's' Data Protection Policy and will act in accordance with it.

I am connected with this organisation in my capacity as a

- ☐ Member of staff
- ☐ Volunteer
- ☐ Trustee/ management committee member

Signature:

Print name:

Date:

Please return this form to **Line Manager to forward to Personnel File.**