

## Data Protection Policy 5.0 – Connections



### Data Protection Policy 5.0

Version	Date	Author	Comments
1.0	Dec 2019	Jules McDonald	Initial version
2.0	Nov 2020	Jules McDonald & Emily Heys	Review
3.0	Jan 22	Jules McDonald & Emily Heys	Review
4.0	June 23	Jules McDonald, Bret McDonald & Emily Heys	Review
5.0	April 2025	Jules McDonald, Bret McDonald & Emily Heys	Review

#### 1. Overview

This policy's goal is to define Connections commitment to data protection.

Connections handle personally identifiable information (PII) about our clients; therefore, information security is something that is taken extremely seriously and the confidentiality, integrity and availability of sensitive data is of the utmost importance.

This policy seeks to ensure that we:

- Comply with data protection laws and best practice.
- Protect ourselves and our clients from risks of data breaches.

Connections operate in accordance with the Data Protection Act of 2018 and the General Data Protection Regulation of 2018 (GDPR) along with all other applicable governmental regulations and legislation.

#### 2. Scope

This policy applies to all the personally identifiable data (PII) that we store and process, regardless of the location of that data.

All Connections' practitioners, and any third-party data processors (e.g., subcontractors), who may be given access to such data must read and abide by this policy. Failure to abide by the policy may result in disciplinary and/or legal action.

### **3. Roles and Responsibilities**

#### **3.1 Data Protection Officer**

##### **Julia McDonald**

The Data Protection Officer ensures the business remains compliant with Data Protection and GDPR laws. The Data Protection Office's responsibilities include:

- Advising the company and practitioners of their obligations.
- Monitoring the company's compliance.
- Addressing potential issues proactively.
- Acting as Connections' point of contact on issues relating to the processing of personal data.
- Responding to enquiries regarding the processing of personal data.
- Co-ordinating a response to actual or suspected breaches in our data.

#### **3.2 Connections Practitioners and Subcontractors**

The appropriate protection of information is required of all practitioners. You are responsible for:

- Adhering to Connections' policies.
- Reporting actual or suspected vulnerabilities to the Data Protection Officer.

### **4. Data Processing Principles**

Per GDPR, the following principles should be followed when processing PII. We require that data be:

- processed lawfully, fairly and in a transparent manner (Lawfulness, fairness, and transparency).
- collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation).
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data minimisation).
- not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation).
- processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage (Security, integrity and confidentiality).

### **5. Data Subjects' Rights**

The subjects of the data have rights in the relation to the way their data is handled under the law, including:

- Where the legal basis of our processing is consent, this consent can be withdrawn at any time.

- Access to the PII we hold can be requested and must be actioned in accordance with GDPR.
- Subjects retain the right to prevent the use of their personal data for direct marketing purposes.
- To ask that data be erased or anonymised in accordance with GDPR.
- To ask us to rectify inaccurate or incomplete data.
- To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.
- To make a complaint to the Information Commissioner's Office.

Requests must be complied with in a timely manner in accordance with GDPR and the Freedom of Information Act.

## 6. Reporting a Breach

As per GDPR we are required to inform the Information Commissioner's Office (ICO) of any breaches of PII where there is a risk to the rights and freedoms of the data subject.

The ICO's data protection self-assessment (<https://ico.org.uk/for-organisations/data-protection-self-assessment/>) can be used to help determine whether a breach requires reporting.

In addition, the breach must be reported to the data subject if it results in a high risk to them.


## 7. Record Keeping

Per GDPR, full and accurate records must be kept reflecting data-processing activities including the data subject's consent and the procedures by which it was obtained.

Records of data breaches must also be kept, detailing the facts of the breach, its effects and immediate and corrective action taken.

## 8. Approval

This policy will be subject to review by the Data Protection Officer. We reserve the right to change this policy at any time without notice.

Authors	Jules McDonald, Bret McDonald & Emily Heys
Date written	December 2019
Date most recently reviewed	1 <sup>st</sup> April 2025
Review Date	April 2026
Print & signed	<div>J McDonald</div>  <div>E Heys</div>

Sheys

B McDonald

B McDonald