



BEACON COUNSELLING TRUST – DATA PROTECTION (GDPR) POLICY & PROCEDURE

Last review completed by	Quality Assurance Team
Date of last review	July 2026
Next review due	July 2027
Approved by Trustees	July 2026

Table of Contents

POLICY	2
1. PURPOSE	2
2. AIMS.....	2
3. SCOPE.....	2
4. LEGAL FRAMEWORK	2
5. ACCOUNTABILITY	2
PROCEDURE	4
1. DOCUMENT MANAGEMENT PROCEDURE	4
2.CONSEQUENCES AND NON-COMPLIANCE	9
3.STORAGE OF RECORDS AND DOCUMENTS.....	4
4. INFORMATION TECHNOLOGY	5
5. DATA BREACH	7
6. PRIVACY POLICIES AND PRIVACY NOTICES	8
7. INFORMATION GOVERNANCE	8
APPENDIX A.....	10
THE DATA PROTECTION ACT.....	10
APPENDIX B	13
OVERVIEW OF THE GENERAL DATA PROTECTION REGULATION (GDPR).....	13
APPENDIX C.....	Error! Bookmark not defined.
SUBJECT ACCESS REQUEST (SAR).....	5
APPENDIX D.....	14
DEFINITIONS.....	16
APPENDIX E	17
DOCUMENT RETENTION SCHEDULE.....	17
APPENDIX F	19
INCIDENT RESPONSE PLAN OVERVIEW.....	19

POLICY

1. PURPOSE

1.1 The Data Protection Policy outlines the responsibilities of Beacon Counselling Trust (BCT) staff in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). As an organisation, we handle sensitive personal data/documents and must ensure they are protected.

2. AIMS

2.1 The policy aims to detail how BCT meets its legal obligations and requirements concerning our requirement to hold data confidentiality and data information security standards.

3. SCOPE

3.1 This policy applies to all employees, board members, and any person contracted or volunteering at BCT.

3.2 The key principles to this policy are:

- Lawfulness, fairness, and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality.
- Accountability.

These are the 7 Key Principles of GDPR.

4. LEGAL FRAMEWORK

This policy is based on the following legislation:

- The General Data Protection Regulation (GDPR).
- The Data Protection Act 2018 (DPA 2018).
- The Data Use and Access 2025

See Appendix A and B

5. ACCOUNTABILITY

5.1 The Board of Trustees holds overall accountability for ensuring BCT complies with data protection legislation.

5.2 Data Protection Officer (DPO) at BCT S. Mitchell is responsible for:

- Informing and advising the charity and its employees about their obligations under data protection laws.
- Monitoring compliance with the GDPR and DPA 2018.
- Managing internal data protection activities.
- Conducting internal audits.
- Providing staff training on data protection.
- Serving as the first point of contact for supervisory authorities and individuals whose data is processed.

5.3 Senior Leadership Team

The Senior Leadership Team are responsible for:

- Implementing appropriate data protection policies and procedures.
- Ensuring staff receive adequate training on data protection.
- Conducting regular reviews of data processing activities.

5.4 All Staff

All staff members are responsible for:

- Complying with this policy and data protection laws.
- Reporting any data breaches or concerns to the DPO immediately.

PROCEDURE

1. DOCUMENT MANAGEMENT

1.1 Data Collection and Processing

- BCT must only collect necessary personal data for legitimate purposes.
- Obtain explicit consent for data processing, except where other lawful bases apply.
- Inform about how their data will be used and for how long it will be retained.

1.2 Data Storage and Security

- Store personal data securely, using encryption where possible.
- Use strong passwords and change them regularly.
- Lock physical files containing personal data in secure cabinets.

1.3 Data Access and Sharing

- Only access personal data necessary for your role.
- Never share personal data with unauthorised individuals or organisations.
- Use secure methods when transferring data electronically.

1.4 Data Subject Rights

- Be prepared to assist with data subject access requests (SARS)
- Know how to handle requests for data rectification, erasure, or restriction.

See Appendix C

1.5 Secure Disposal

When documents and records reach the end of their retention periods, they must be securely disposed of:

- Paper records should be shredded using secure destruction and recycling in a Shred-it container.
- Electronic records should be permanently deleted and, where possible, drives should be securely wiped.
- Seek guidance from the DPO when unsure.

See Appendix D and E

1.6 Breach Reporting

- Report any suspected data breaches immediately to the DPO.

2.STORAGE OF RECORDS AND DOCUMENTS

2.1 Tangible Records – Tangible records that *do not* contain confidential information are those that can be physically moved to storage, such as paper records (including printed versions of electronically saved documents), photographs, investor presentations, and promotional items etc. These active, tangible records and documents, which need to be easily accessible, may be stored in BCT office space or equipment.

2.2 Confidential Information

Records and documents that contain Confidential Information but are in use should be stored in the locked storage of the responsible individual accountable for them.

2.3 Clean Desk

All employee desktops should be organised in a manner whereby only material currently in use or to be immediately used should be visible. In the event of an employee having extended periods away from his/her/their desk, Public Information is neatly organised in folders, and Strictly Confidential Information should be locked away. Each employee shall be provided with at least one lockable drawer/cabinet to store documents that should be kept off their desktop. All confidential information shall be kept out of view from unauthorised personnel and locked up when not in use.

2.4 Home and Off-Site Use of Printed Confidential Documents

It is every employee's responsibility, in accordance with data protection legislation, to protect the confidential information of our business, its employees, partners and . Confidential documents printed for use at home or off-site must be kept secure and out of sight of unauthorised individuals at all times. Printing should be limited to what is necessary, with documents securely stored when not in use, and either returned to BCT premises or confidentially destroyed once no longer required. If an employee is accessing and printing company files on a home or off- site computer, all computer security software must be up-to-date and effective. Any loss, unauthorised access or breach must be reported immediately in line with BCT procedures.

2.5 Inactive documents

Inactive documents containing personal data are securely stored with our commissioners / ICT providers, and reviewed periodically, and disposed of/ or anonymised when no longer required, in line with GDPR principles. Further information regarding Document Retention Schedules can be found in Appendix E.

2.6 Legal and Financial Regulations

Please note that in some jurisdictions and domains, human resource, legal, and financial documents may have specific rules and regulations governing their retention, distribution, storage, and destruction. Please contact the DPO in the first instance for any specific information, directions, and practices regarding those documents. Further information regarding Document Retention Schedules can be found in Appendix E.

3. INFORMATION TECHNOLOGY

3.1 Data Protection by Design Technology in as much as:

None of the BCT trustees are data protection professionals; Trustees, with guidance from the Clinical Director will seek appropriate professional advice corresponding with its data protection requirement whenever:

- They are planning to make significant changes to the ways in which they process personal data.
- If there is any national publicity about new risks (for example a cyber-attack).
- Any material changes to the UK-GDPR are proposed or have been made, which might adversely compromise BCT legitimate processing of personal data covered by the UK-GDPR.
- Personal data will never be transmitted electronically (e.g. by e-mail) unless securely encrypted.

4. SUBJECT ACCESS REQUEST (SAR)

Under the provision of the Data Protection Act an individual can request access to their personal information regardless of the media in which this information may be held / retained. This person is known as the Data Subject.

4.1 Acknowledgment

BCT must acknowledge the SAR as soon as possible and ask for identification before progressing with this request (see Appendix C for SAR Form). If the SAR is made by someone other than the person the data is about (such as a friend, relative or solicitor), BCT must check that this person is authorised to have such information. BCT will require written authority from the Data Subject that the person in question can act on their behalf, or if applicable, a document showing general power of attorney.

4.2 Data Subject Request

BCT must check what information the Data Subject has requested. Before considering giving them their information, the staff member who is dealing with the enquiry must thoroughly check that any information released does not relate to anyone else. For example, if there is an email that mentions a number of different people, the staff member must 'redact' (black out) any information which **doesn't** relate to the person making the SAR. The actions detailed in this section must be made in conjunction with the DPO.

4.3 Record Keeping

BCT must keep dated records of the information that has been sent to the Data Subject for future reference, for example if the Data Subject is unhappy with the response or makes another request soon after.

4.4 Timeline

BCT must give a copy of the data they hold about the Data Subject as soon as possible, and no later than within 1 calendar month of the request. See [Time limits for responding to data protection rights requests | ICO](#) for further information.

In certain circumstances, for example particularly complex or multiple requests, BCT can take a further 2 months to provide data. In this case, they must tell the individual:

- Within 1 month of the request.
- Why there is a delay.

4.5 When information can be withheld

There are some situations when BCT will be allowed to withhold information, for example if the information is about:

- The prevention, detection, or investigation of a crime.
- National security or the armed forces.
- The assessment or collection of tax.
- Judicial or ministerial appointments.

BCT does not have to say why they are withholding information.

- BCT has a legal obligation to comply with all appropriate legislation in respect of data, information, and information security. It also has a duty to comply with the guidance issued by the Information Commissioner (ICO).
- All legislation relevant to an individual's right of confidence and the ways in which that can be achieved and maintained are paramount to BCT. BCT are aware that penalties could be imposed upon BCT, and/or BCT employees for non-compliance with relevant legislation.

For more information see [Getting copies of your information \(SAR\) | ICO](#)

5. DATA BREACH

5.1 What is Data Breach?

A data breach is any incident involving accidental or unlawful loss, misuse, alteration, unauthorised disclosure of, or access to personal data. All data breaches must be reported immediately, investigated, and recorded in line with BCT's procedures.

A data breach could happen if someone's personal information is:

- Inappropriately accessed.
- Lost.
- Accidentally destroyed.
- Altered without permission.
- Damaged.
- Disclosed to someone it shouldn't have been.

5.2 Responsibility

BCT is responsible for personal information and however accidental, a breach could have a negative impact on a person's livelihood and wellbeing. It should be noted that some data breaches won't cause any harm beyond possible inconvenience. The type of breach will facilitate decision-making about whether or not BCT need to notify the relevant supervisory authority or the affected individuals, or both.

5.3 Informing the Data Protection Officer

In the event of any data breach coming to the attention of the Data Controller (DC) S. Keatley and the Trustees, they will liaise immediately with the DPO and Caldicott Guardian (S. Mitchell). This ensures confidential information about is used ethically, legally, and appropriately, and will determine the context of the risk and if necessary, notify the Supervisory Authority and Information Commission's Office (ICO) within 72hours.

5.4 Investigations

If full details of the nature and consequences of the data breach are not immediately accessible, BCT will bring that to the attention of the ICO and undertake to forward the relevant information as soon as it becomes available. The DPO will ensure investigation takes place immediately and internal reporting procedures are in place which includes an Incident Response Plan (IRP overview see Appendix F) which will be used in all Data Incidents.

5.5 High Risk Breach

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the UK GDPR states BCT must inform those concerned directly and without undue delay. A 'high risk' means the requirement to inform individuals is higher than for notifying the ICO. BCT will need to assess both the severity of the potential or actual impact on individuals as a result of a breach, and the likelihood of this occurring. In such cases if the risk is higher, BCT will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. If a decision is made not to notify individuals, BCT will need to notify the ICO, unless it is demonstrated that the breach is unlikely to result in a risk to rights and freedoms. BCT will document any decision-making processes in line with the requirements of the accountability principle and will keep a record of any personal data breaches, regardless of whether they are required to notify. Further Information can be found at [Personal data breaches: a guide | ICO](#).

6. PRIVACY POLICIES AND PRIVACY NOTICES

6.1 BCT has a Privacy Policy and appropriate Privacy Notices are available to everyone on whom it holds and processes personal data, in accordance with 1.1(procedure). These documents are available on the BCT website at [Beacon Counselling Trust](#). In the case of data obtained directly from the data subject, the Privacy Notice will be provided at the time the data is obtained. In the case that the data is not obtained directly from the data subject, the Privacy Notice will be provided within a reasonable period of BCT having obtained the data (within one month), or, if the data is used to communicate with the data subject, at the latest, when the first communication takes place; or if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

6.2 Data Complaints

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details provided. If you remain unhappy with how we've used your data after raising a complaint with us. The complaint should provide as much detail as possible and should be sent to:

Support@beaconcounsellingtrust.co.uk or [263 Townsend Lane, Liverpool L13 9DG](#)

The complaint will be acknowledged within 30 days of receiving and will be recorded securely and necessary to investigate. Complaints will then be managed by the Data Protection Officer (DPO) who will handle the response and share the outcome without undue delay. Complaints should be made to BCT before escalating a complaint to the **Information Commissioner's Office (ICO)**. Website: <https://www.ico.org.uk/make-a-complaint>

7. INFORMATION GOVERNANCE

Information Governance is defined as the way an organisation manages, protects, and uses information responsibly, ensuring compliance with legal, ethical, and security requirements.

While some of the points below are detailed throughout this policy, they complement and reinforce BCT commitment to managing all information securely, lawfully, and ethically by

- Ensuring compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Common Law Duty of Confidentiality, and the Human Rights Act 1998, as well as NHS standards such as the Caldicott Principles where applicable. This applies to all information, including personal, sensitive, and organisational records, whether paper-based, electronic, or verbal.
- Ensuring all staff, trustees, volunteers, contractors, and placement students handle information responsibly.
- Ensuring access to personal and sensitive data is restricted to those who require it to perform their role, and information must only be used for lawful and relevant purposes.
- Ensuring data is stored securely and only shared outside BCT when there is a legal, contractual, or consent-based reason.
- Ensuring compliance is regularly monitored through audits and reviews, and staff are supported with guidance and refresher training to maintain high standards of information protection across the organisation.
- Ensuring that everyone handling information receives training on their responsibilities, including maintaining confidentiality, keeping data accurate, and reporting any suspected breaches immediately.

With this in mind all staff are required to complete annual Information Governance and Data Protection training. Training will be completed when staff, volunteers and trustees join the organisation and then refresher training at suitable intervals.

Training will cover confidentiality, secure handling of personal data, individual rights, breach reporting, phishing awareness and role-specific responsibilities.

BCT's framework includes a relevant and up to date suite of policies, established accountabilities and responsibilities, and guidance, processes and training for our staff, will ensure effective Information Governance.

8. CONSEQUENCES AND NON-COMPLIANCE

8.1 Failure to comply with this policy and procedure may result in disciplinary action and, in severe cases, legal consequences for both the individual and BCT. Implementation of and compliance with the policy is essential to its effectiveness. Each employee must understand and cooperate in the implementation and enforcement of the Policy.

All Policies and Procedures can be translated into the appropriate language

APPENDIX A

THE DATA PROTECTION ACT

The Data Protection Act 2018 controls how your personal information is used by BCT.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using your personal data must follow strict rules called 'data protection principles. We must make sure the information is:

- Used fairly, lawfully, and transparently.
- Used for specified, explicit purposes.
- Used in a way that is adequate, relevant, and limited to only what is necessary.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary.
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

There is stronger legal protection for more sensitive information, such as:

- Race.
- Ethnic background.
- Political opinions.
- Religious beliefs.
- Trade union membership.
- Genetics.
- Biometrics (where used for identification).
- Health.
- Sex life or orientation.

There are separate safeguards for personal data relating to criminal convictions and offences (see safeguarding adults policy for further information).

YOUR RIGHTS

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- Be informed about how your data is being used.
- Access personal data.
- Have incorrect data updated.
- Have data erased.
- Stop or restrict the processing of your data.
- Data portability (allowing you to get and reuse your data for different services).

- Object to how your data is processed in certain circumstances.

You also have rights when an organisation is using your personal data for:

- Automated decision-making processes (without human involvement).
- Profiling, for example to predict your behaviour or interests.

There is a requirement to make the public, who use the service of BCT, aware of why BCT needs information about them, how this is used and to whom it may be disclosed.

Specific information must be given to about the use of their personal information, particularly if for uses other than the provision of healthcare. The explicit consent of the Service User is normally obtained before information is processed for reasons other than the direct provision of healthcare. Under the GDPR there are certain conditions whereby information may be processed without consent. BCT will only do this if:

- The information is necessary for the direct healthcare of .
- We have received explicit consent from individuals to be able to use their information for a specific purpose.
- There is an overriding public interest in using the information e.g., to safeguard an individual, or to prevent a serious crime.
- There is a legal requirement that will allow us to use or provide information (e.g., a formal court order or legislation).
- A breach of the Data Protection requirements could result in a member of staff facing disciplinary action. All staff must ensure they are aware of and adhere to BCT policies and procedures relating to the processing of personal information.
- Whilst there is a public expectation of appropriate sharing of information between organisations providing health care services to them and with other organisations providing related services, the public rightly expects that their personal data will be properly protected. Information sharing protocols provide the basis for facilitating the exchange of information between organisations. Under the GDPR each organisation must ensure that, where information processing is undertaken, that appropriate technical and organisational security measures have been put in place to adequately protect the data they are processing.

DATA ACT 2025

The Data Use and Access Act 2025 (DUAA) is a summary of the changes to data protection law that affect if BCT as an organisation using personal information.

What data protection laws does the DUAA change?

The DUAA amends, but does not replace, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR).

The DUAA helps BCT to innovate in the following ways:

- **Research provisions:** it makes it clearer when BCT can use personal information for the purposes of scientific research, including commercial scientific research. It clarifies that people can give 'broad consent' to an area of scientific research.
- **Privacy notices:** it allows BCT to re-use people's personal information for scientific research without giving them a privacy notice, if that would involve a disproportionate effort. So long as BCT protect their rights in other ways and still explain what we are doing by publishing the notice on our website.
- **Automated decision-making:** it opens up the full range of reasons, or 'lawful bases', that BCT rely on when using people's personal information to make significant automated decisions about them. So long as BCT continue to apply appropriate safeguards. This potentially includes allowing BCT to rely on the legitimate interests lawful basis for this type of processing. This doesn't apply to special category data which is more protected.
- **Cookie rules:** it allows you to set some types of cookies without having to get consent, such as those you may use to collect information for statistical purposes and improve the functionality of your website.

For further information please see [The Data Use and Access Act 2025 \(DUAA\) - what does it mean for organisations? | ICO](#)

APPENDIX B

OVERVIEW OF THE GENERAL DATA PROTECTION REGULATION (GDPR).

The GDPR seeks to harmonise data protection legislation across Europe. The approach of the GDPR is to ensure that companies providing services or goods are required to comply with the GDPR should they process (hold, obtain, record, use or share) and information pertaining to an EU citizen.

The GDPR sets out specific rights of individuals and affirms that proactively organisations must assure themselves as to the use of, transfers of, and legal basis for processing of all the information they hold. Further, where new uses or processes for information are introduced, these must be subject to a Data Protection Impact Assessment, and in certain circumstances, approval must be obtained by the supervisory authority (for BCT that is the Information Commissioner) before that processing may commence.

This legislation applies to all people with identifiable information held in manual files, computer databases, videos, and other automated media, about living individuals. The legislation dictates that information should only be disclosed on a need-to-know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty. Any unauthorised disclosure of information by a member of staff may result in disciplinary action.

The legislation also requires BCT (where appropriate) to register its information held manually and on computers and other automated equipment with the Information Commissioners' Office, identifying the purposes for holding the data, how it is used and to whom it may be disclosed. Failure to register (where appropriate), an incorrect registration or an outdated registration, are criminal offences, which may lead to prosecution of BCT. BCT notification is maintained and reviewed annually.

APPENDIX C

DATA PROTECTION SUBJECT ACCESS REQUEST FORM

*indicates required information

Use this form to request personal information that **Beacon Counselling Trust (BCT)** holds about you. Please only ask for the information you need and give as much detail as possible to help us locate your information.

Part A

Title:*

Surname:*

Forename(s):*

Date of Birth:*

dd/mm/yyyy

Email address:*

Current address line 1:*

Current address line 2:

Current address line 3:

Current postcode:*

Please indicate below your previous address if applicable.

Previous address line 1:

Previous address line 2:

Previous address line 3:

Previous postcode:

Part B

Please indicate below the type of records that you wish to have access to. Asking for specific information and supplying details, rather than asking for all your information, may help us to process your request faster or provide the right information.

- A specific piece of information or information relating to a specific interaction or event (please supply details in Part C)
- Other (Please supply details in Part C)

Please tell us the range of your information request to cover.

Start Year 06/04/????:*

End Year 05/04/????:*

Part C

IMPORTANT: Please enter in the space below the following information:

- As much detail as possible about any specific information you require.
- Any other details you feel will assist us in tracing and retrieving your information.

Further details:

Part D

I declare that I am the person named in Part A and that I am entitled to request personal information under the terms of the Data Protection Act 2018.

- I agree with the above declaration*

Date:

DD/MM/YYYY

Part E

Proof of ID - Provide a photo or scanned copy of a birth certificate, driving license or passport.

Proof of address - Provide a photo, original digital version or scanned copy of a bank statement, utility bill, council tax bill or TV license.

APPENDIX D

DEFINITIONS

Documents and Records (used interchangeably) refer to all business records of BCT, including written, printed, as well as electronic records (i.e., e-mails and documents saved electronically). Documents and records include but are not limited to papers, copies, drafts, bound records, drawings, maps, photographs, electronic communications, and any other physical device containing information, including Electronic Storage Devices. The term includes all copies or originals taken, moved, or sent off to any BCT premises and within BCT control.

Confidential Information – all information that is produced during BCT business that is not available from public sources is considered confidential. In general, any or all documents or files that contain business, service user, partner or employee names, pricing, personal information. This includes, but is not limited to,

Service user information, Assessments, Session Sheets, Wage Information, Invoices, Letters to and from BCT, any printed material that refers to BCT or our partners and .

This also includes private information on individuals as defined by the Data Protection Act (DPA 2018) and the General Data Protection Regulation (GDPR 2018), as well as information that is available to our company as a result of our business practice(s) but which is not generally known or readily obtainable by others outside of our business, but can be used in general throughout our business.

General Business Information – General business information documents including, but not limited to:

Accounting documents Information technology documents General Contracts Customer lists Internal reports Payroll statements Training information and manuals Executive level budgets Customer correspondence Legal contracts Strategic reports Health and safety records Medical records Payroll information Performance appraisals	Corporate legal records Supplier purchase orders Supplier records Supplier specifications Research and development reports Performance appraisals Product testing and results Product development plans Sales and marketing reports Specifications and drawings Internal communications Advertising materials Business strategies
--	---

Electronic Storage Device - refers to all electronic storage devices that were provided by or contain information that is the property of BCT, are under BCT control, and are used by any of its employees, contractors, officers, or directors. Electronic Storage Devices include personal computers, servers, laptops, and related storage devices such as hard drives, flash drives, and CDs.

APPENDIX E

DOCUMENT RETENTION SCHEDULE

(Updated January 2026)

DOCUMENT RETENTION SCHEDULE

Records and information should only be retained when there is a business need to do so. Under UK GDPR and the DPA 2018 personal data processed by BCT must not be retained for longer than is necessary for its lawful purpose. Information held for longer than is necessary carries additional risk and cost.

Here is a list of documents that contain confidential information. These recommendations are guidelines only. They are not intended to represent legal advice. For further advice BCT would need to contact legal expert(s) or government or regulatory authority to ensure we are following current legal requirements for our area.

TYPE OF RECORD/SPECIFIC RECORD	RETENTION PERIOD
Accounting Records	6 +1 years
Annual financial statements	6 +1 years
Data for acquired/divested business	6 +1 years
Monthly financial statements	6 +1 years
General ledger	6 +1 years
Annual audit records	6 +1 years
Journal entries	6 +1 years
Cancelled cheques	6 +1 years
A/P paid invoices	6 +1 years
Business expense records	6 +1 years
Data for non-acquired/non-divested	6 +1 years
Data Processing Agreement	6 +1 years
Accounts payable	6 +1 years
Accounts receivable	6 +1 years
Audit reports	6 +1 years
Expense records	6 +1 years
Loan documents, Purchase orders	6 +1 years

Sales records	6 +1 years
Bank reconciliations	6 +1 years
Tax Records	6 +1 years
PAYE records	6 +1 years
Purchasing and Sales	6 +1 years
Purchase Orders, Requisitions	6 +1 years
Sales Contracts, Sales Invoices	6 +1 years
Insurance Records	6 +1 years
Policies (including expired)	2 years
Claims for loss/damage,	6 +1 years
Accident reports, appraisals	5 years
Settled Insurance Claims	6 +1 years
Legal and Workplace Records	5 years
General Contracts	5 years
Premises contracts & records	5 years
Personnel	5 years
Attendance Records	5 years
Client / Service User Records	6 + 1 year
Contracts	5 years
Disability, Employment Applications	5 years
Performance Records – After	5 years
Terminations	5 years
Personnel Files – Terminated	5 years
SMS – Client / Service User text message correspondence	90 Days
Building inspection reports (e.g. boilers; heating	6 + 1 year
Equipment monitoring and testing and maintenance work	10 years
Risk Registers	6 + 1 year
Visitors sign in books	2 years
Fire evacuation drill books / logs	2 years
Formal complaints about discrimination by/within the organisation	10 years
Complaints Records (including correspondence, investigation and outcomes)	10 years
Whistle Blowing record	6 months

General Declarations of Interests / Conflicts of Interest Register	6 + 1 year
Gifts and Hospitality Register	6 + 1 year

S. Mitchell is designated with the responsibility and authority to file, store, and/or archive the information outlined above.

Any challenges to the retention of personal data must be considered in accordance with [GDPR Article 17 \(Right to erasure\)](#), or the equivalent sections in the [DPA 2018](#) if the processing is for law enforcement purposes. The right to erasure does not apply where we are legally obliged to process personal data or where the processing is necessary for performing our functions.

APPENDIX F

INCIDENT RESPONSE PLAN OVERVIEW

Overview: Incident Response Plan

