

Data Protection Policy (GDPR)

What is GDPR

Under current legislation on data protection, almost all charities should have a Data Protection Policy. The Data Protection Policy is an internal statement of how our organisation protects the personal data it processes. This policy will be reviewed annually.

1. Data protection principles

The Beds and Northants MS Therapy Centre, hereafter referred to as the Centre, is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals;
- b. 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 shall not be considered to be incompatible with the initial purposes;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. accurate and, where necessary, kept up to date; every reasonable step 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;
- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes 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; and
- f. 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."

2. General provisions

- a. This policy applies to all personal data processed by the Centre.
- b. The Manager and Trustees shall take responsibility for the Centre's ongoing compliance with this policy.
- c. This policy shall be reviewed at least annually.

d. The Centre shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Centre shall maintain a Register of Systems.

b. The Register of Systems shall be reviewed at least annually.

c. Individuals have the right to access their personal data and any such requests made to the Centre shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the Centre must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).

b. The Centre shall note the appropriate lawful basis in the Register of Systems.

c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Centre's systems.

5. Data minimisation

a. The Centre shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. The Centre shall take reasonable steps to ensure personal data is accurate.

b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Retention

- a. To ensure that personal data is kept for no longer than necessary, please refer to the retention document (Appendix A)

8. Security

- a. The Centre shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- c. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Centre shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website) at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

Appendix A

Retention of Documentation

| Purchase invoices and supplier documentation | | |
|---|--|--|
| Document | Retention period | Reason for retention period |
| Payments cash book or record of payments made | Six years from the end of the financial year in which the transaction was made | Companies Act/Charities Act ¹ |
| Purchase ledger | | Companies Act/Charities Act |
| Invoice - revenue | | Companies Act/Charities Act |
| Petty cash records | | Companies Act/Charities Act and HMRC |
| Invoice - capital item | Ten years | Companies Act/Charities Act and HMRC |
| Successful quotations for capital expenditure | Permanently | Commercial considerations |
| Income / Monies Received | | |
| Document | Retention period | Reason for retention period |
| Bank paying in counterfoils | Six years from the end of the financial year in which the transaction was made. | Companies Act/Charities Act |
| Bank Statements | | Companies Act/Charities Act |
| Correspondence re. Donations | | Companies Act/Charities Act |
| Bank Reconciliations | | Companies Act/Charities Act |
| Receipts cash book | | Companies Act/Charities Act and HMRC |
| Sales Ledger | | Companies Act/Charities Act and HMRC |
| Deeds of covenant / Gift Aid declarations | Six years after the last payment made. Twelve years if payments outstanding or dispute regarding the deed | Data Protection Act |

| | | |
|----------|--|---------------------|
| Legacies | Six years after the estate has been wound up | Data Protection Act |
|----------|--|---------------------|

| Payroll Documentation | | |
|---|---|--|
| Document | Retention period | Reason for retention period |
| Income tax records re. employees leaving i.e: P45 | Six years plus current year | Taxes Management Act |
| Notice to employer of tax code (P6) | Six years plus current year | Taxes Management Act |
| Annual return of employees and Directors expenses and benefits (P11D) | Six years plus current year | Taxes Management Act |
| Certificate of pay and tax deducted (P60) | Six years plus current year | Taxes Management Act |
| Notice of tax code change | Six years plus current year | Taxes Management Act |
| Annual return of taxable pay and tax deducted | Six years plus current year | Taxes Management Act |
| Records of pensions deductions (including superannuation) | Six years plus current year | Pensions Act |
| Payroll and payroll control account | Six years plus current year | Companies Act / Charities Act and Taxes Management Act |
| | | |
| Employee / Personal Records | | |
| Document | Retention period | Reason for retention period |
| Accident Books, accident reports, reports | Three years after last entry or end of investigation if later | The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 |
| Details of medical schemes | Permanently | Commercial |
| Organisational Charts | Permanently | Commercial |

| | | |
|--|--|---|
| Personnel Files and training records | Six years after employment ceases | Limitations Act 1980 |
| Wages and salary records | Six years plus the current year | Taxes Management Act |
| Expense accounts/records | | Taxes Management Act |
| Overtime records/authorisation | | Taxes Management Act |
| Redundancy details, calculations of payments, refunds, notifications to the Secretary of State | Six years after employment has ceased | Data Protection Act |
| Application Forms and Interview Notes for unsuccessful candidates | Six months to a year | Disability Discrimination Act 1995 and Race Relations Act 1976 recommend six months. One year limitation for defamation actions under Limitations Act |
| Statutory Maternity Pay Records, calculations, certificates or other medical evidence | Three years after the end of the tax year in which maternity period ends | The Statutory Maternity Pay Regulations |
| Statutory Sick Pay records, calculations, certificates, self-certificates | Three years after the end of the tax year in which Statutory Sick Pay period ends | Statutory Sick Pay (General) Regulations |
| Records relating to working time | Two years from date on which they were made | The Working Time Regulations |
| National minimum wage records | Three years after the end of the pay reference period following the one that records cover | National Minimum Wage Act |
| Members Consent Forms | 7 years plus current year | |
| Members medical records | 7 years plus current year | |

Buildings, Plant and Engineering

| Document | Retention period | Reason for retention period |
|-----------------|--|------------------------------------|
| Deed of Title | Permanently or until property is dispose of. Copy of deeds should be kept for six years after disposal | Data Protection Act |
| Leases | Fifteen years after expiry | Limitations Act 1960 |

| | | |
|---|--|---|
| | | |
| Final plans, designs and drawings of the building, planning consents, building certifications, collateral warranties, records of historical interest and final health and safety file | Permanently or until six years after property is disposed of | Data Protection Act |
| Asbestos Register and Asbestos Disposal Certificate | Permanently. Property holders are required to examine the premises for asbestos or possible asbestos materials, record the location and those materials and assess the risk. These assessments are to be recorded and provided to anyone who may disturb the asbestos. | Control of Asbestos at Work Regulations |
| Hazardous substances: disposal of heavy metals and radioactive sources | Permanently | Data Protection Act |
| Plant and Machinery | Until one year after the plant and machinery is removed from the building | Data Protection Act |

Pension Records

| Document | Retention period | Reason for retention period |
|---|---|---|
| Details re. current pensioners | Ten years after benefit ceases | Commercial |
| Pension scheme – next of kin/expression of wish forms | Six years after date of death | Data Protection Act |
| All Deeds and rules | Permanently | Companies Act, Commercial, Pensions Act |
| Trustees Minute Book | Permanently | Companies Act, Commercial, Pensions Act |
| Annual Accounts | Permanently | Companies Act, Commercial, Pensions Act |
| Pension scheme investment policies | Twelve years from the ending of any benefit payable | Companies Act, Commercial, Pensions Act |

| | | |
|---|--|---|
| Actuarial Reports | Permanently | Companies Act, Commercial, Pensions Act |
| Contribution Records | Permanently | Companies Act, Commercial, Pensions Act |
| Insurance Documents | | |
| Document | Retention period | Reason for retention period |
| Policies | Three years after lapse | Data Protection Act |
| Claims correspondence | Three years after settlement | Data Protection Act |
| Employer's Liability Insurance Certificate | Forty years | Employers' Liability (Compulsory Insurance) Regulations 1988 |
| Accident reports and relevant correspondence | Three years after settlement | Data Protection Act |
| Other Documents | | |
| Document | Retention period | Reason for retention period |
| Trustee/Director/Trustee Minutes of meeting and decisions | Permanently | Data Protection Act |
| Annual Accounts and annual review | Permanently | Data Protection Act |
| Major agreements of historical significance | Permanently | Data Protection Act |
| Investment Certificates | Permanently | Companies Act, Charities Act, Commercial |
| Health and Safety Records | Three years for general records. Permanently for records relating to hazardous substances | Personal Injury actions must generally be commenced within three years of injury. However, industrial injuries not capable of detection within that period eg. Asbestos, the time period may be substantially extended. |
| Investment Ledger | Permanently | Companies Act, Charities Act, Commercial |

| | | |
|--|--|--|
| Fixed Asset Register | Permanently | Companies Act, Charities Act, Commercial |
| Contract with customers, suppliers or agents, licensing agreements, indemnities and guarantees and other agreement or contract | Six years after expiry or termination of the contract. If the contract is executed as a deed, the limitation period is twelve years. | Limitations Act 1980 |