Data Protection Policy (including data retention & security)

Policy statement/purpose

Malvern Special Families needs to gather and use certain information about individuals.
These can include enquirers, applicants, customers (our families – parents/carers, children and young people), suppliers, employees and other people and organisations Malvern Special Families has a relationship with or may need to contact.
This policy describes how this personal data will be collected, handled, stored, how long it will be retained and how it will be disposed of to meet the organisation's data protection standards and to comply with the law.

Scope of the policy

This data protection policy ensures Malvern Special Families:

- Complies with data protection law and follows good practice
- Aligns to the seven general data protection regulation principles
- Is transparent about how it stores and processes individuals' data
- Protects itself from the risk of a data breach
- Protects the rights of staff, volunteers, customers, suppliers and partners.
- In addition to safeguarding the rights of data subjects this policy will also ensure that excessive amounts of data are not retained unnecessarily by Malvern Special Families and aims to improve the speed and efficiency of managing data.

These include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision-making including profiling

Roles and Responsibilities

This policy applies to:

- Admin office of Malvern Special Families
- All MSF Clubs
- All staff
- All contractors, suppliers and other people working on behalf of or in partnership with Malvern Special Families

It applies to all data that the organisation holds relating to living, identifiable individuals, even if that information technically falls outside of the Data Protection Act and any and all subordinate legislation made thereunder. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Photos
- Any other information relating to individuals identified under the Data Protection Act.

Everyone who works for or with Malvern Special Families has responsibility for ensuring that data is collected, stored and handled appropriately.
Each team that handles personal data must ensure that it is managed and processed in line with this policy, data protection principles and local protocols.

However, the following roles have key areas of responsibility:

The **Trustee Board** sets policy so that Malvern Special Families meets it legal obligations. It also checks and approves any contracts or agreements with third parties that may handle sensitive data.

The **Leadership Team (Business Manager & Service Manager)** are the Data Owners and ultimately accountable for delivering the policy so that Malvern Special Families meets its legal obligations

Staff managing teams or processes have a Data Stewardship responsibility ensuring teams and processes are compliant with the data protection framework

The **Data Protection Officer (Business Manager)** is responsible for:

- Monitoring compliance with the General Data Protection Regulation
- Reviewing all data protection procedures and related policies, in line with an agreed schedule
- Keeping the Trustee Board updated about data protection responsibilities, risks and issues
- Reviewing data protection impact assessments
- Cooperating with the supervisory authority and acting as a contact point
- Auditing the record of Malvern Special Families data processing operations

Malvern Special Families **Trustee Board** has a service agreement with a specialist IT company and are responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services Malvern Special Families uses to store and process data

Principles

- Personal and sensitive data will be kept accurate and up to date
- The only people able to access data covered by this policy will be those who need it to carry out their work. This will be managed via a contractual obligation or solutions such as role based access control
- Data will not be shared informally or disclosed to unauthorised people, either within the organisation or externally
- Malvern Special Families will provide training and support to all employees to help them understand their responsibilities when handling data
- Employees will keep all data secure, by taking sensible precautions and following guidelines
- Data will only be stored securely as defined in the process guidance issued by the Information Commissioner's Office.
- Strong passwords will be used and they will never be shared
- Data will be regularly reviewed and updated if it is found to be out of date. If it has reached the end of its retention period, it will be deleted and securely disposed of
- Data will be securely backed up
- Data must be password encrypted before being transferred electronically or via removable media (CD, DVD, USB etc.)

- Personal data will never be transferred outside of the European Economic Area without appropriate approval
- Data will not be retained longer than is necessary

All individuals who are the subject of personal data held by Malvern Special Families are entitled to:

- Have access to their personal data and supplementary information processed and held by Malvern Special Families
- Request a copy of their information
- Be informed how to keep any information held up to date
- Be informed how the organisation is meeting its data protection obligations

In certain circumstances, known as exemptions or derogations, the Data Protection Act allows personal data to be disclosed without the consent of the individual. Under these circumstances Malvern Special Families may disclose the requested data. Prior to disclosure, we will ensure the request is legitimate.

Data use

Personal data is of no value to Malvern Special Families unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- Employees must ensure the screens of their computers are always locked when unattended
- Personal data must not be shared informally. In particular, it should never be sent in the body of any email as this form of communication is not secure and open to sharing with the wrong party
- The Business Manager will offer support and explain how to send data to authorised external contacts
- Employees must not save copies of personal data to their own computers. Always access and update the central copy (Cloud based) of any data.
- All data stored in electronic form, and in particular personal data, should be stored securely using passwords.
- All data stored in hardcopy format or electronically on removable physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.
- Personal data should not be taken from the Childcare Provision without agreement for transport and storage. They must never be left attended in cars or opened on public transport. If it is necessary to take them home due to not returning to the Childcare Provision, they must be stored in a lockable box at all times and returned to the Childcare Provision at the earliest opportunity.
- All paper based personal data (including files, or duplicate copies of information) that are no longer needed at the Childcare Provision should be shredded on site or returned securely to the office where they will be shredded.
- No data, and in particular personal data, should be transferred to any computer or mobile device (including but not limited to laptops, tablets, smartphones) personally belonging to an employee, unless in exceptional circumstances with the formal written approval of the Business Manager and in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.
- Personal data may only be transferred to devices belonging to agents, contractors or other parties working on behalf of Malvern Special Families where the party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR.

Malvern Special Families aims to ensure that individuals are aware that their data is being processed and that they understand:

- Who the data controller is
- The purpose or purposes and legal basis/bases for which information will be processed
- Categories of personal data
- Any recipient or categories of recipients of the personal data
- Details of transfers to countries outside of economic union and appropriate safeguards

- Retention period or criteria used to determine the retention period
- The existence of each of data subject's rights
- The right to withdraw consent at any time, where relevant
- Their right to complain to the Information Commissioner's Office
- The source the personal data originates from and whether it came from publicly accessible sources
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences

Using images of children

We may take photographs of the children at our clubs and events. We may use these images in individual children's Journals (a record of their journey through our Clubs), our club prospectus or in other printed publications that we produce, as well as on our website or on social media. We may also make video recordings, for monitoring, publicity or other educational use.

From time to time, our clubs may be visited by the media who will take photographs or film footage of a special event. The children and young people will often appear in these images, which may appear in local or national newspapers, or on televised news programmes.

To comply with the Data Protection Act we need parental/carer permission before we can photograph or make any recordings a child.

MSF have an information sharing section in the parent contract available to all parents and carers and consents issued to parents when they complete the annual Registration forms.

Data Disposal

Upon the expiry of the data retention periods set out in Appendix 1 attached to this policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed or otherwise disposed of as follows:

- Personal data stored electronically shall be deleted
- Personal data in hardcopy form shall be shredded

Data Retention

As stated above, and as required by law, Malvern Special Families shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

Different types of personal data, used for different purposes, will necessarily be retained for different periods **(**and its retention periodically reviewed), as set out in Appendix 1.

When establishing and/or reviewing retention periods, the following shall be taken into account:

- The objectives and requirements of Malvern Special Families
- The type of personal data in question
- The purpose(s) for which the data in question is collected, held, and processed
- Malvern Special Families legal basis for collecting, holding, and processing that data
- The category or categories of data subject to whom the data relates

If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

Notwithstanding the following defined retention periods, certain personal data may be deleted or

otherwise disposed of prior to the expiry of its defined retention period where a decision is made by the Trustee Board to do so (whether in response to a request by a data subject or otherwise).

Definitions

For the purposes for the General Data Protection Regulations, Article 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 lists the definitions

Equality and diversity

We are committed to respecting diversity in all aspects of our work and we will not tolerate any form of discrimination.

Recording and monitoring

The success of the application of this policy will be measured by the level of data protection compliance within Malvern Special Families. This will be measured by the Business Manager undertaking quarterly audits within the organisation. This will be used, alongside discussion of Data Protection at every Trustee meeting to keep the Trustee Board updated about data protection responsibilities, risks and issues.

Commitment & review

The policy will be reviewed at least annually and/or whenever there are changes to data protection legislation.

The Trustee Board looks to the support and professionalism of staff at all levels in making this policy truly effective. The effectiveness of this general statement of intent and other specific policies and procedures in use, will be regularly reviewed and revised as and when necessary.

Approved by the Trustee Board of Malvern Special Families Dated 11 June 2018

APPENDIX 1 – DETAILS OF DATA RETENTION PERIODS

Type of record	Retention Period	Retention Guidance Source
Children's records including registers, medication records, CYP files, accident/incident forms, photos, risk assessments, behaviour support plans Child Protection Records	Until the child reaches the age of 25yrs DOB + 25yrs	*EYFS Welfare Requirements, Childcare Act 2006, Limitation Act 1980/The Statute of Limitations Act 1991.* *WSCB*
Records of any **reportable death**, injury, disease or dangerous occurrence	3 years after the date on which it happened	*The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR*
Personnel files including application forms and training records including disciplinary records, working time records, health details, references Child Protection allegation details made against staff,/Trustees, even if unfounded	6 years after employment ceases Until persons normal retirement age or 10yrs from date	*Chartered Institute of Personnel and Development* *WSCB*
DBS Check – proof of ID	6 months	*DBS Code of Practice.* The DBS Certificate is issued ONLY to the individual on whom the check was carried out. We will retain the following information from the DBS certificate: the name of the subject, the date of issue of a Disclosure the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure
Application forms and interview notes for unsuccessful candidates	6 months to 1 year	*Chartered Institute of Personnel and Development*
Wage/salary records including overtime, bonuses and expenses	6 years	*Taxes Management Act 1970*
Statutory Maternity Pay (SMP) records	3 years after the end of the tax year in which the maternity period ends	*The Statutory Maternity Pay Regulations 1986*
Statutory Sick Pay (SSP) records	3 years after the end of the tax year to which they relate	*The Statutory Sick Pay (General) Regulations 1982*
Income tax and National Insurance returns/records	At least 3 years after the end of the tax year to which they relate	*The Income Tax (Employments) Regulations 1993*
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy	*Chartered Institute of Personnel and Development*
Staff accident records	3 years after the date of the last entry	*Social Security (Claims and Payments) Regulations 1979* ***The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980.***
Accident/medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)1999	40 years from the date of the last entry	*The Control of Substances Hazardous to Health Regulations 1999 (COSHH)*
Assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	Permanently	*Chartered Institute of Personnel and development*
Accounting records	6 years	**Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006.**
Complaints record book	At least 3 years from the date of the last record	*Early Years Foundation Stage Welfare Requirements given legal force by Childcare Act 2006*
Insurance liability documents	40 years from date of issue	*The Employers' Liability (Compulsory Insurance) Regulations 1998*
Minutes/minute books **Trustee meeting minutes & AGM** **Annual Reports** **Business Plans** **Contracts information – including funding contracts**	10 years from the date of the meeting Permanently End of contract period + 6yrs	Companies Act 2006 CIPD The Limitation Act 1980
Visitors Log	2 Years	