Data Protection Policy (including data retention & security)
Last reviewed Feb 26

Policy statement/purpose
Malvern Special Families (MSF) 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 MSF:

- 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 MSF 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 MSF
- All MSF Clubs
- All staff
- All contractors, suppliers and other people working on behalf of or in partnership with MSF

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 MSF 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 MSF meets it legal obligations. It also checks and approves any contracts or agreements with third parties that may handle sensitive data.

The **Leadership Team (CEO & Service Manager)** are the Data Owners and ultimately accountable for delivering the policy so that MSF 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 (CEO)** 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 MSF data processing operations

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
- MSF 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 (USB, portable hard drive 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 MSF are entitled to:

- Have access to their personal data and supplementary information processed and held by MSF
- Request a copy of their information - Subject Access Request (SAR)
- 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 MSF may disclose the requested data. Prior to disclosure, we will ensure the request is legitimate.

Data use

Personal data is of no value to MSF 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 CEO 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 CEO 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 MSF where the party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR.

MSF 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, MSF 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 MSF
- The type of personal data in question
- The purpose(s) for which the data in question is collected, held, and processed
- MSF 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 MSF. This will be measured by the CEO 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 annually and/or whenever there are changes to data protection legislation.

MSF does not need to be registered with the Information Commissioner's Office (ICO).

Approved by the Trustee Board of Malvern Special Families
Dated June 2018
Review - October 25
Latest Review Feb 26

APPENDIX 1 – DETAILS OF DATA RETENTION PERIODS

Type of record	Retention Period	Status	Retention Guidance Source	Disposal
CHILDREN'S RECORDS				
Attendance registers	Requirement is 6 years after child has left the setting. Recommended is 26 years.	Requirement Recommended	Data Protection Act and UK GDPR	Secure Disposal
Accident Records Over 18 years at time of incident	3 years	Requirement	Social Security (Claims and Payments) Regulations 1979 Regulation 26 Social Security Administration Act 1992 Section 8 Limitation Act 1980 (Section 11)	Secure Disposal
Accident Records Under 18 years at time of incident	DOB + 22 years	Requirement	Limitation Act 1980 (Section 11)	Secure Disposal
Accident/medical records as specified by the Control of Substances Hazardous to Health Regulations **(COSHH)** 2002	40 years from the date of the last entry	Requirement	The Control of Substances Hazardous to Health Regulations 2002(COSHH)	Secure Disposal
Children - Records of any **reportable death**, injury, disease or dangerous occurrence, Accident/incident records and risk assessments specific to child. Full record of notifications to statutory agencies.	DOB + 26yrs	Recommendation	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR	Secure Disposal
Children's records • medication records (on regular medication) • CYP files including parent/carer contract • risk assessments, • behaviour support plans • care plans	DOB + 26yrs	Requirement	Childcare Act 2006, Limitation Act 1980/The Statute of Limitations Act 1991. Data Protection Act and UK GDPR WSCB	Secure Disposal
Children's Records related to Welfare & safeguarding: • A child is seriously injured • A child is on regular medication • A child has severe allergies • A child has a serious illness	DOB + 26 years For Looked After Children 75 years	Requirement	Limitation Act 1980, The Statute of Limitations (Amendment) Act 1991 Working Together to Safeguard Children, updated July 2022 Keeping Children Safe in Education, updated September 2023	Secure Disposal
Child Protection allegation details made against staff/Trustees, even if unfounded.	Until the alleged perpetrator reaches normal retirement age, or for 10 years, whichever is the longer.	Requirement	Safeguarding and child protection guidance For private, voluntary, and independent early years and childcare providers. June 2023	Secure Disposal
Bound & Numbered Book Positive Physical Intervention Team Teach record book	75 years from the date of the last record	Requirement	Sue Stokes - Director of PBT Ltd.	Secure Disposal

Other records which may contain personal information or images of children, parents and carers. • Photographs • Websites • Socia media posts • Texts • Emails • Apps • Cloud storage	Keep permissions given by parent/carers for 21 years and 6 months	Recommendation	Professional Association for Childcare and Early Years 2018	Secure Dispoasl
STAFF & EMPLOYMENTRECORDS				
Staff files including • application forms • references • training records • disciplinary records • supervisions, appraisals • working time records, • health details • qualifications	Duration of employment + 7 years	Recommendation	Chartered Institute of Personnel and Development Under GDPR any staff can request "the right to be forgotten" but we have an obligation to keep this data and should not erase it until the 7-year retention period has expired. UK GDPR 2018	Secure Disposal
DBS Check – proof of ID	6 months	Recommendation	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	Secure Disposal
Evidence of Right to Work in the UK	Duration of employment + 2 years	Recommendation	An employer's guide to right to work checks (Home Office)	Secure Disposal
Application forms and interview notes for unsuccessful candidates	6 months to 1 year	Recommendation	Information Management Toolkit for schools, 2019 Chartered Institute of Personnel and Development	Secure Disposal
Wage/salary records **Timesheets** including overtime, bonuses and expenses	6 years after the end of the tax year to which the records relate. Current year + 6 years	Recommendation	Taxes Management Act 1970 Information Management Toolkit for Schools, 2019	Secure Disposal

Statutory Maternity Pay (SMP) records	3 years after the end of the tax year in which the maternity period ends	Requirement	The Statutory Maternity Pay Regulations 1986, revised 1999	Secure Disposal
Sickness Absence Monitoring	Where sickness pay is not paid then current year + 3 years If sickness pay is made then it becomes a financial record and current year + 6 years applies	Requirement	The Statutory Sick Pay (General) Regulations 1982 Information Management Toolkit for Schools, 2019	Secure Disposal
Statutory Sick Pay (SSP) records	3 years after the end of the tax year to which the records relate	Requirement	Information Management Toolkit for Schools, 2019	Secure Disposal
Income tax and National Insurance returns/records	At least 3 years after the end of the tax year to which they relate	Requirement	The Income Tax (Employments) Regulations 1993	Secure Disposal
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy	Recommendation	Chartered Institute of Personnel and Development Information Management Toolkit for Schools, 2019	Secure Disposal
Risk Assessments – premises, trips etc.	Life of the Risk Assessment + 3 years provided that a copy is stored with the accident report if an incident has occurred.	Recommendation	Information Management Toolkit for Schools, 2019	Secure Disposal
Staff accident records	3 years after the date of the last entry		Social Security (Claims and Payments) Regulations 1979, Regulation 26. Limitation Act 1980. (Section 11)	Secure Disposal
Staff records relating to Accident or Injury at Work	Date of incident + 12 years. Serious accidents will have a further retention period applied	Recommendation	Information Management Toolkit for Schools, 2019	Secure Disposal
Operational Administration				
Assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	Permanently	Recommendation	Chartered Institute of Personnel and development	Secure Disposal
Accounting records	6 years	Recommendation	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006.	Secure Disposal
Complaints record Records relating to complaints made to and investigated by provider	Serious complaints: current year + 6 years. If negligence involved: current year + 15 years. If child protection or safeguarding issues are involved: current year 40 years.	Recommendation	Information Management Toolkit for Schools, 2019 Childcare Act 2006	Secure Disposal
Employer Insurance liability Certificates	Closure of setting + 40 years	Requirement	The Employers' Liability (Compulsory Insurance) Regulations 1998 Information Management Toolkit for schools, 2019	Secure Disposal
Insurance Documents **Including Inventories of furniture and equipment**	6 years after the year to which the information relates	Recommendation	Information Management Toolkit for schools, 2019	Secure Disposal
Minutes of staff and room meetings	Date of meeting + 3 years then review	Recommendation	Information Management Toolkit for Schools, 2019 There may be data protection issues if minutes refer to individual children and staff members.	Secure Disposal
Trustee meeting minutes & AGM **Annual Reports**	10 years from the date of the meeting Permanently	Recommendation	Companies Act 2006 CIPD	Secure Disposal

Business Plans				
Contracts information – including funding contracts	End of contract period + 6yrs	Recommendation	The Limitation Act 1980	Secure Disposal
Visitors Log	Current year + 6 years	Recommendation	Information Management Toolkit for schools, 2019	Secure Disposal
Fire Logs	Current year + 3 years	Recommendation	Information Management Toolkit for schools, 2019	Secure Disposal
Correspondence created by management	Date of Meeting + 3 years	Recommendation	Information Management Toolkit for schools, 2019	Secure Disposal