ST NICHOLAS TRAINING CENTRE FOR THE MONTESSORI METHOD OF EDUCATION LTD (MSN, CHARITY) AND
ST NICHOLAS MONTESSORI TRAINING LIMITED
(MONTESSORI CENTRE INTERNATIONAL – MCI, COLLEGE)
LONGACRE CHILDCARE LTD (LCL)
"(together, "Montessori")"

Data Protection Policy

1. Introduction

MSN, MCI and LCL needs to retain and process certain data in order to enable the efficient running of the business. This includes certain personal data of our employees, students and other contacts for a variety of purposes. When processing information, we are committed to protecting the rights and privacy of all our personal data in compliance with the Data Protection Act 1998 (the 'Act') and related legislation. This Policy sets out the principles that will apply in meeting this commitment. Throughout this document where it refers to the Charity or MSN it also includes MCI and LCL.

2. In summary the Data Protection Act state that personal data shall:

Under the Data Protection legislation there are certain responsibilities in relation to personal data held on computers and also certain manual records where they form part of a structured filing system. Under the regulations, all personal data is subject to the 'eight data protection principles. All employees must be aware of and act in accordance with the principles.

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the rights of employees.
- Be kept safe from unauthorised access, accidental loss or destruction.

3. The Data Controller and the Designated Data Controllers

3.1 The Charity as a body corporate is the Data Controller under the 1998 Act, and the Trustees are therefore ultimately responsible for implementation of the Policy. However, the Designated Data Controller will deal with day-to-day matters who will be responsible for monitoring our compliance with data protection principles as well as the effectiveness of this policy. MSN has appointed Director of Operations for the role.

3.2 Any member of staff, student, applicant, customer or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself should raise the matter with the Designated Data Controller.

4. Responsibilities of employees

4.1 All staff are required to:

- Take practical steps to comply with the principles, ensuring personal data is never left visible or unattended on a desk, photocopier or computer screen;
- Never disclose personal information about another member of staff, student, customer, external colleagues or supplier;
- Be responsible for the preservation of the confidentiality and integrity of information during the course of your work;

4.2 If and when, as part of their responsibilities, staff collect personal information about other people (e.g. employees or other people such as students, external colleagues or suppliers), you must comply with this policy including the data protection principles and guidelines set out in the Data Protection Code of Practice.

5 Data Security

5.1 All staff are responsible for ensuring that:

- Any personal data that is hard copy should be kept in a locked filing cabinet or drawer;
- If it is computerised, all work is to be saved on the network drive, which is backed up every day, in specific folders that only certain staff (who are working with this data) have access to or document is password protected;
- If a copy is kept on a removable storage media, that media must itself be kept in a locked filing cabinet or drawer;
- Confidential personal information is not disclosed to anyone except the data subject, unless the data subject has given their explicit prior written consent to this. You verify the identity of the individual and the legitimacy of the request before releasing any personal information;
- Passwords are to be strong and not shared with others (unless working on the same data) and that passwords are kept separate from laptops and phones;
- When working on personal information as part of your role when away from your workplace, you continue to follow the terms of this policy, in particular in relation to data security.

5.2 Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct.

6 Processing Sensitive Information

6.1 Sometimes it is necessary to process information about a person's health and criminal convictions. This may be to ensure that MSN is a safe place for everyone, or to operate other policies, such as the sick pay policy or the equal opportunities policy. Because this information is considered sensitive under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent to process this data. An offer of employment or a course place may be withdrawn if an individual refuses to consent to this without good reason.

6.2 MSN holds personal data to carry out our legal duties under the employment contract including payroll and benefits administration and to ensure we can carry out our general business and HR activities. Information about employees should only be published where:

- There is a legal obligation to do so, and/or;
- The information is clearly not intrusive, and/or;
- The individual has consented to the disclosure.

Where the member of staff gives their consent they should be made aware of the extent of information that will be published, how it will be published and the implications of this.

6.2 All staff have a right to access certain personal data being kept about them either on computer or in certain files. Any member of staff who wishes to exercise this right should complete the Subject Access Request Form and submit it to the appropriate Designated Controller (see above).

7 Rights to Access Information

Anyone whose personal data is being processed by MSN has certain rights in relation to their personal data. In practice, what this means is that individuals have the right, on written request and within a **month** to:

- Know what personal data is being processed about them, why it is being processed, where it came from and to whom it may be disclosed;
- Know how to keep it up to date or rectify if the data is inaccurate;
- Restrict processing;
- Not to be subject to automated decision-making, for example in recruitment selection;
- Know what MSN is doing to comply with its obligations under the 1998 Act;
- Gain access to personal data by completing the Subject Access Request Form and submit it to the Designated Controller.

8. Subject Consent

8.1 In many cases, MSN can only process personal data with the consent of the individual. In some cases, if the data is sensitive as defined in the 1998 Act, express consent must be obtained. Agreement to MSN processing some specified classes of personal data is a condition of acceptance, for example a student onto any course, a child into a setting and a condition of employment for staff. This includes information about previous criminal convictions.

8.2 Some jobs or courses will bring the applicants into contact with children, including young people. MSN has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job, and students for the courses offered. MSN also has a duty of care to all staff and students and must therefore make sure that employees and those who use MSN facilities do not pose a threat or danger to other users.

8.3 MSN may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. MSN will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example. The application form that all prospective staff and students are required to complete will include a section requiring consent to process the applicant's personal data.

9. Retention of Data

MSN has a duty to retain some staff and student personal data for a period of time following their departure from the organisation, mainly for legal reasons, but also for other purposes such as being able to provide references and academic transcripts, or for financial reasons, for example relating to pensions and taxation. Different categories of data will be retained for different periods of time. The exact details of retention periods and purposes are set out in Appendix 1.

10. Conclusion

Compliance with the 1998 Act is the responsibility of all members of MSN. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or to access to the facilities of MSN being withdrawn, or even to a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the appropriate Designated Data Controller.

Policy reviewed May 2018
Approved: October 2016

Appendix 1 – Retention of personal data by MSN

Type of Record	Location of Storage	Retention Period	Reason for Length of Period
Personal staff files including references, CVs, appraisal forms, training records, notes of disciplinary and grievance hearings.	Secure server and locked filing cabinet for paper records	6 years from the end of employment or contract	References and potential litigation
		Certain personal data may be held in perpetuity	Selected material form part of the official MSN Archive
Facts relating to redundancies where 20 or more redundancies	Secure server and locked filing cabinet for paper records	12 years from the date of redundancy	Time limits on litigation Limitation Act 1980
Recruitment Application forms/ interview notes	Secure server and locked filing cabinet for paper records	At least 6 months from the date of the interview	Time limits on litigation
Income Tax and NI Returns, including correspondence with tax office	Secure server and locked filing cabinet for paper records	At least 3 years after the end of the financial year to which the records related	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	Secure server and locked filing cabinet for paper records	At least 3 years after the end of the financial year to which the records related	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	Secure server and locked filing cabinet for paper records	At least 3 years after the end of the financial year to which the records related	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	Secure server and locked filing cabinet for paper records	6 years	Taxes Management Act 1970
Accident books and records and reports of accidents	Secure server and locked filing cabinet for paper records	3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985
Health Records	Secure server and locked filing cabinet for paper records	During employment (staff) During course (students)	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment/course is connected with health, including stress related illness	Secure server and locked filing cabinet for paper records	3 year	Limitation period for personal injury claims
Student application records for those who are rejected or who decline an offer	Secure server and locked filing cabinet for paper records	No more than 4 months after the start of the academic year	Permits institution to handle enquiries from the data subject

Student records of those not completing enrolment	Secure server and locked filing cabinet for paper records	Within one academic year	Permits institution to handle delayed enrolments
Student records, including enquiries, applications, admissions ,assessment, awards, attendance and conduct	Secure server and locked filing cabinet for paper records	At **least 6 years** from the date that the student leaves the institution, in case of litigation for negligence, where information is available	Limited period of negligence
	Secure server and locked filing cabinet for paper records	At least 10 years for personal academic references	Permits institution to provide references for a reasonable length of time
	Secure server and locked filing cabinet for paper records	Certain personal data may be held in perpetuity	While personal and academic references may become 'stale', some date, e.g. transcripts of student marks may be required throughout the student's future career. Upon the death of the data subject, date relating to him/her ceases to be personal data. Some selected material will form part of the official College Archive.
Assessment evidence	Secure server, secure online fileshare (eg. Dropbox)	Until learner has qualified and EQA has had an opportunity to review evidence	This evidence is primarily held and shared with MSN by approved centres. It must be retained until all quality assurance procedures have been satisfactorily completed.
Assessment & monitoring records - EQA Reports, IQA Reports, Assessment feedback, Attendance/Notes from meetings	Secure server	3 years	This may be required for audit by Crossfields Institute and LMU (the regulator). The only personal data should be names and signatures.
Individual learner and staff logins for the virtual learning environment (VLE) – this requires first and last name and email address	How To Moodle Hosted to a dedicated server, GDPR Compliant.	For the duration of the course and indefinitely thereafter unless removed requested by learner or the course is	This allows learners to continue to access resources as long as they are made available.
Mailing list membership (first and last names and email address)	Mailing list membership (first and last names and email address) GDPR compliant	Indefinite, receiver can request to opt-out at any time	Consent is required to join a mailing list, and there is always an option to unsubscribe