Data Protection Policy

1. Policy Statement

This policy notice has been written to comply with the EU General Data Protection Regulation (GDPR). MY Schools Together needs to gather and use certain information about individuals. These can include pupil information, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

The Act protects the rights of individuals whom the data is about (data subjects), mainly by placing duties on those who decide how and why such data is processed (data controllers). Data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

MY Schools Together are registered with Information Commissioner as a data controller and we ensure that any processing of personal data for which we are responsible complies with the Act. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

This policy describes how we meet our obligations when collecting, handling and storing personal data. Protects the rights of staff, volunteers, service users and partners and protects itself from the risks of a data breach

2. Definitions

The Data Protection Act defines the word “data” as information which:

(a) Is being processed by means of equipment operating automatically in response to instructions given for that purpose

(b) Is recorded with the intention that it should be processed by means of such equipment,

(c) Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or

(e) Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

Personal data - is all data which relates to identifiable individuals, such as job applicants, current and former employees, volunteers, clients, suppliers and marketing contacts. Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title.

Data Protection Policy

Sensitive personal data - is personal Data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings. Any use of sensitive personal data will be strictly controlled in accordance with this policy.

Relevant filing system (referred to in paragraph (c) is defined in the Act as:

any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Accessible record (referred to in paragraph (d)) means:

a health record that consists of information about the physical or mental health or condition of an individual, made by or on behalf of a health professional in connection with the care of that individual; an educational record that consists of information about a pupil, which is held by a local education authority or special school or an accessible public record that consists of information held by a local authority for housing or social services purposes

3. The Principles

The Data Protection Act describes how organisations must collect, handle and store personal information, these rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The Data Protection Act is underpinned by eight important principles; these say that personal data must:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Obligations

MY Schools Together meet the requirements of the act when collecting, handling and storing personal data.

4.1 Purpose

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes. The purposes for which personal data may be used by us includes; personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice;
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests;
- Ensuring business policies are adhered to (such as policies covering email and internet use);
- Investigating complaints;
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments;
- Monitoring staff conduct, disciplinary matters;
- Marketing our business and services;
- Improving services;
- Contacting service users and/or their parents/carers (and in case of emergencies) ;
- Obtaining consent from service users (and parents/carers) to participate in projects and activities;
- Obtaining consent from service users (and parents/carers) to take photographs and to use photographs for marketing purposes;
- Having accurate medical records for service users in case of accident and/or incidents.

4.2 Data accuracy

MY Schools Together takes reasonable steps to ensure data is kept accurate and up to date and data will be updated as inaccuracies are discovered.

4.3 Data storage

Data is stored safely and securely and access is restricted to authorised personnel only - as specified in the Information Security Policy.

4.4 Data protection breaches

MY Schools Together have procedures in place to help prevent data security risks and a Data Protection Breach Procedure all breaches are recorded and reported on a Data Protection Breach Procedure - Reporting Form.

4.5 Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, MY Schools Together will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

4.6 Providing information

MY Schools Together aims to ensure that individuals are aware that their data is being processed, and that they understand; how the data is being used and how to exercise their rights. MY Schools Together Privacy Notice is given to individuals at the time their personal data is collected.

4.7 Subject access requests

All individuals who are the subject of personal data held by MY Schools Together are entitled to:

- Ask what information the school holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the Data Protection Officer at: DPO@oldham.gov.uk MY Schools Together will always verify the identity of anyone making a subject access request before handing over any information.

5. Responsibilities

Everyone who works for or with MY Schools Together has some responsibility for ensuring data is collected, processed, stored and handled appropriately. Individuals that handle personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the governors are ultimately responsible for ensuring that MY Schools Together meets its legal obligations and the key areas of responsibility listed below:

5.1 The Director's responsibilities

The governors have overall responsibility for the day-to-day implementation of this policy and for the organisations data protection responsibilities, risks and issues including;

- Reviewing all data protection procedures and policies on a regular basis;
- Arranging data protection training and advice for all staff members and those included in this policy;
- Answering questions on data protection from employees and volunteers;
- Responding to individuals who wish to know which data is being held on them by MY Schools Together (subject access requests);
- Checking and approving with third parties that handle the company's data any contracts or agreements regarding data processing;
- Ensure all systems, services, software and equipment meet acceptable security standards;
- Checking and scanning security hardware and software regularly to ensure it is functioning properly;
- Researching third-party services, such as cloud services the company is considering using to store or process data;
- Approving data protection statements attached to emails and other marketing copy;
- Addressing data protection queries from clients, target audiences or media outlets;
- Ensuring all marketing initiatives adhere to data protection laws and the company's Data Protection Policy.

5.2 Employees responsibilities

High-profile security breaches have increased public concern about the handling of personal information. As some 80% of security incidents involve staff there is a clear need for all workers to have a basic understanding of the Data Protection Act 1998 (DPA).

This section outlines the responsibilities which staff are expected to follow:

- Employees should keep all data secure, by taking sensible precautions. In particular, strong passwords must be used and they should never be shared;
- To lock/log off computers when away from their desks;
- To prevent virus attacks by taking care when opening emails and attachments or visiting new website;
- To ensure personal data is not left on desks, and securely storing hard copy personal information when it is not being used;
- Positioning computer screens away from windows to prevent accidental disclosures of personal information;

- To encrypt personal information that is being taken out of the office if it would cause damage or distress if lost or stolen;
- Data should not be shared or disclosed to unauthorised people, either within the company or externally;
- To request help from the data protection officer if they are unsure about any aspect of data protection;
- To collect only the personal information they have been instructed to collect;
- To explain new or changes to data collection to service users and to obtain consent or provide an opt-out where appropriate;
- Never disclosing customer personal information over the telephone, to prevent these disclosures they should carry out identity checksbefore giving out personal information to someone making an incoming call;
- To pass on the contact details of the Data Protection Officer if they receive a subject access requests;

6. Additional Information

Both Mather Street & Yew Tree (MY Schools Together) are registered with the Information Commissioner's Office under registration reference:

Mather Street School -

Yew Tree Community - **Z7135123**

For more information on registration, the General Data Protection Regulation (GDPR) or the Data Protection Act visit the Information Commissioner's Office website available at: www.ico.org.uk/