Mesne Lea Primary School

Working together for individual excellence

Policy for Data Protection

Authorised by	Governing Body
Review date	October 2020
Equality Impact Assessed	Model Policies EIA by Salford LA

Introduction

Salford City Council is fully committed to compliance with the requirements of the Data Protection Act 2018 ("the Act") and the General Data Protection Regulation (GDPR), which came into force in May 2018. The council will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under data protection legislation.

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO has the power to impose enforcement action on organisations in the UK.

Statement of Policy

In order to operate efficiently, Salford City Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within legislation to ensure this. Salford City Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the council and those with whom it carries out business. The council will ensure that it treats personal information lawfully and correctly.

To this end the council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 2018.

The Principles of Data Protection

The Act stipulates that anyone processing personal data must comply with **Six Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information is:

1. used fairly, lawfully and transparently
2. used for specified, explicit purposes
3. used in a way that is adequate, relevant and limited to only what is necessary
4. accurate and, where necessary, kept up to date
5. kept for no longer than is necessary
6. handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Lawful Bases for Processing Personal Data

Processing is only lawful if there is a lawful basis to do so. The lawful bases for processing are set out in Article 6 of the GDPR. The council will ensure that at least one of these will apply whenever personal data is processed:

(a) Consent: the individual has given clear consent for their personal data to be processed for a specific purpose.
(b) Contract: the processing is necessary for a contract with the individual.
(c) Legal obligation: the processing is necessary for the council to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for the council to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply to public authorities processing data to perform official tasks.)

Policy Scope

This policy refers to data protection legislation, which provides conditions for the processing of any data defined as **personal data and/or "special category" personal data**.
Personal data is defined as data relating to a living individual who can be identified from:
 That data;

 That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Special Category personal data is defined as personal data consisting of information as to:

Racial or ethnic origin;

 Political opinion;

 Religious or other beliefs;

 Trade union membership;

 Physical or mental health or condition;

 Sexual life;

 Biometrics (where used for identification);

There are separate safeguards for personal data relating to criminal convictions and offences – see Article 10 of the GDPR.

Handling of Personal/Special Category Data

Salford City Council will, through appropriate management and the use of strict criteria and controls:-

- Fully observe conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

These include:

- The right to be informed;
- The right of access to one's personal information;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling

If an individual makes a request relating to any of the rights listed above, the council will consider each request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for complying with such a request unless the request is deemed to be unnecessary, excessive in nature, or a repeated request.

All subject access requests must be answered within 1 month of the day after receipt. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. The council will notify the data subject of any such extension within one month of receipt of the request together with the reasons for the delay. All requests received for access to, or deletion/rectification of personal data must be directed to infogovernance@salford.gov.uk.

In addition, Salford City Council will ensure that:

- There is specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;

Everyone managing and handling personal information is appropriately supervised;

 Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;

 Queries about handling personal information are promptly and courteously dealt with;

 Methods of handling personal information are regularly assessed and evaluated;

 Performance with handling personal information is regularly assessed and evaluated;

 Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures. All elected members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All managers and staff within the council's directorates will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

 Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;

 Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;

 Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other servants or agents of the Council must:
 Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the council, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the council and that individual, company, partner or firm;

 Allow data protection audits by the council of data held on its behalf (if requested);

 Indemnify the council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by the council will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the council.

Data Protection Responsibilities

In compliance with the GDPR, the council has an appointed Data Protection Officer (DPO). The DPO, working with the Corporate Information Governance Team (CIGT), has overall responsibility for monitoring internal compliance, informing and advising on data protection obligations, and acts as a contact point for data subjects.

The DPO is responsible for ensuring:
 this Policy is implemented;

 the provision of data protection training for staff within the council;

 for the development of best practice guidelines;

 for carrying out compliance checks to ensure adherence with data protection legislation throughout the authority.

Notification of Data Breaches

The council employs a robust information security incident management process. All staff are obliged to report any incidents involving information to the CIGT to ensure they are dealt with.

A data breach is a type of information security incident where the confidentiality, integrity or availability of personal data has been affected. In accordance with the GDPR, the council will report qualifying data breaches (defined below) to the ICO **within 72 hours**.

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Information Commissioner Registration

The ICO maintains a public register of data controllers and data protection officers. Salford City Council is registered as such.

The Data Protection Act 2018 requires every data controller, who is processing personal data, to notify and renew their notification on an annual basis. Failure to do so is a criminal offence.

This policy has been reviewed and approved by the Governing Body at Mesne Lea School.

Signed_____ Name _____

Head Teacher

Signed_____ Name _____

Chair of Governors