DATA PROTECTION AND CONFIDENTIALITY

PERSON RESPONSIBLE FOR POLICY:	**Claire Mallia**
APPROVED: GOVERNING BODY	**DATE:** NOVEMBER 2020
SIGNED:	**ROLE:**
TO BE REVIEWED:	**SPRING 2021**

LINCOLN GARDENS PRIMARY SCHOOL

Data Protection and Confidentiality Policy

1.Introduction

Lincoln Gardens Primary School aims to ensure that all personal data it holds in respect of pupils and their families, staff, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018

This policy applies to all personal and sensitive data, regardless of whether it is in paper or electronic format.

The DPA and GDPR apply to personal information processed by organisations such as the council. To operate efficiently we have to collect and use (process) personal information about the individuals. We take compliance with the Data Protection legislation very seriously. The school is registered as a data controller with the information Commissioner's Office; registration number Z8162107.

As Data Controllers for the personal information we hold, we are liable for enforcement action from the Information Commissioner's Office (ICO) for non-compliance with Data Protection legislation. This could include a monetary penalty up to £500,000 under the Data Protection Act and up to £18 million under the General Data Protection Regulation. Liability could extend to individual employees in certain circumstances, such as if personal information were to be unlawfully obtained or disclosed and this could result in disciplinary action or a personal fine.

The school publishes a Privacy Notice to parents annually in respect of the personal information we control and process about their child/ren. The Privacy Notice sets down how we use that information and who we share it with and for what purpose. We are responsible for compliance with the content of this notice at all times.

The aim of this policy is to set out how we will comply with the DPA and the GDPR when processing personal information.

Scope

This policy applies to all pupils at Lincoln Gardens Primary School, parents, staff, governors and visitors to the school.

Definitions

Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics

	• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

How the Data Protection Act Applies

In the Data Protection Act the word 'data' means information that:

- Is processed automatically;
- Is recorded with the intention that it will be processed automatically;
- Is recorded as part of a relevant filing system or with the intention of being part of such as system;
- Does not fall within the above three categories but which forms part of an accessible record, such as health records, educational records (local education authority and special schools only), local authority housing records and local authority social service records;
- Is recorded and held by a public authority which does not fall within the above four categories.

A *'relevant filing system'* is one where information is organised either by reference to individuals or by criteria relating to individuals so that a specific detail about a person may be easily selected from the system.

Personal Data is that which could identify someone either directly or indirectly.

Sensitive Personal data under the DPA is defined as data about: racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences.

When does the GDPR Apply?

Under GDPR Personal Data means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

The GDPR refers to sensitive personal data as "special categories of personal data". Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Principles of the GDPR

We have a duty under the GDPR, unless an exemption applies, to comply with six legally enforceable principles. Data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Processed in a manner that ensures appropriate security of the personal data.

Compliance with the Data Protection Act & the GDPR

We will, through appropriate management, ensure that anyone authorised to access personal information takes appropriate care by:

- Observing the conditions regarding the fair and lawful collection and use of personal information;
- Specifying the legal basis, purpose and condition for processing for the personal information being processed and by not using this information for another incompatible purpose unless we have notified data subjects prior to any such change.
- Collecting and processing only the appropriate amount of information needed to fulfil operational needs or to comply with any legal requirements;
- Ensuring the quality of personal information created, used and held;
- Keeping personal information secure;
- Applying strict checks to determine the length of time personal information should be held and ensuring it is not kept for longer than is necessary or disposed of too soon;
- Ensuring that individuals are aware of their rights under the DPA 2018 and GDPR
- Only applying exemptions as permitted by the DPA and the GDPR.
- Ensuring that any third parties contracted by the school to process personal data adhere to appropriate controls and that appropriate checks are carried out to ensure compliance;
- We will not transfer any data outside the European Economic Area (EEA).
- Investigating and responding to complaints in relation to the DPA and GDPR, as set out in the Complaints Policy.
- Investigating and responding to security incidents and possible data breaches as set out in our Security Incident and Data Breach Protocols.

The rights of individuals under the Data Protection Act

The DPA provides individuals with certain rights, as below:

1. Request a copy of their personal information - these requests are known as 'Subject Access Requests' or 'SARs' and further information can be found in the Schedule 05A Access to Information Policy.

2. Request that inaccurate information be rectified, erased, destroyed or blocked – information will be amended or deleted or a note will be attached explaining why this is not possible.

3. Prevent processing for direct marketing – if the school carries out direct marketing these activities will stop in response to a request from an individual.

4. Prevent automated decision taking – if the school is making a significant decision about an individual just using automated means individuals have the right to request human input. (Please be aware that the school does not employ automated means for any decision making purposes)

5. Seek compensation - an individual, who suffers material damage or distress as a result of the councils not complying with the DPA principals, is entitled to seek compensation if it can be demonstrated that reasonable care to comply was not taken.

In addition, individuals have rights under GDPR as follows:

- 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;

- Rights in relation to automated decision making and profiling.

6. Sharing personal data

We will only normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Records of Processing

The GDPR requires the school to demonstrate compliance with the legislation. Our Privacy Notices states Records of Processing for all instances where personal data is processed by the council to explain how and why the data is being processed. The Record of Processing template is shown as Appendix A.

Privacy Notices

Under DPA there is the requirement for the council to be transparent about personal data processed by putting Privacy Notices in place to explain about this processing.

There is a general Privacy Notice on the council's website. Additional more specific Privacy Notices are created and these are clearly stated where necessary on written literature, council web pages and verbally, if individuals are being spoken to face to face or by telephone.

Under the GDPR the information that must be included within Privacy Notices is set out in the legislation.

6. Privacy by Design

The councils have adopted Privacy by Design and Default principles that mean privacy requirements and Data protection compliance are taken into account as part of day to day work and during projects when processes are being designed and systems implemented. The Privacy Impact Assessment process explained in the next section is used to assess privacy risk and to aid compliance with Data Protection legislation.

7. Privacy Impact Assessments & Data Protection Impact Assessments

Privacy Impact Assessments (PIAs) are carried out as part of the Integrated Impact Assessment process on major council decisions and projects if personal information is involved and there are risks to the privacy of individuals and to non-compliance with the DPA.
The following questions are considered when deciding whether or not to carry out a PIA:

1. Will new personal information be collected?
2. Will personal information be disclosed to organisations or people who have not previously had access to the information?
3. Will personal information be used for a purpose it is not currently used for, or in a way it is not currently used?
4. Is new technology to be used that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition technology?
5. Will decisions be made or action taken about individuals in ways that can have a significant impact on them?
6. Is personal information involved that is particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be extremely private.
7. Will individuals be contacted in ways that they may find intrusive?

The PIA Template in Appendix C will be used to carry out the assessment and record the results.

Under GDPR these assessments will be known as Data Protection Impact Assessments. This policy will be updated when full details are known.

Data Protection Audit

Under GDPR there is a requirement for the school to carry out audits to understand the obligations that must be complied with to identify any gaps.

How to contact the Information Commissioner

Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; Telephone: 0303 123 1113 or 01652 545700;
Email: notification@ico.gsi.gov.uk; Web: www.ico.gov.uk