



Lambley Primary School
Data Protection Policy

Approved by	F G B and C O'Hara Link Governor
Date Approved	13.11.2018
Version	1
Review Date	Nov2019



Lambley Primary School Data Protection Policy

May 2018

Lambley Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue Privacy Statement to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulation May 2018 and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

What we must do:

1. All employees must **comply** with the requirements of Data Protection Law and Article 8 of the Human Rights Act when processing the personal data of living individuals
2. Where personal data is used we must make sure that the data subjects have access to a complete and current **Privacy Notice**.
3. We must formally **assess** the risk to privacy rights introduced by any new (or change to an existing) system or process which processes personal data
4. We must process only the **minimum** amount of personal data necessary to deliver services.
5. All employees who record **opinions** or intentions about service users must do so carefully and professionally

Due regard been given to Equalities Act legislation

6. We must take reasonable steps to ensure the personal data we hold is **accurate**, up to date and not misleading.
7. We must rely on **consent** as a condition for processing personal data only if there is no relevant legal power or other condition
8. Consent must be obtained if personal data is to be used for **promoting or marketing** goods and services.
9. We must ensure that the personal data we process is reviewed and **destroyed** when it is no longer necessary.
10. If we receive a **request** from a member of the public or colleagues asking to access their personal data, we must handle it as a **Subject Access Request**
11. If we receive a request from anyone asking to access the personal data of **someone other than themselves**, we must fully consider Data Protection law before disclosing it
12. When someone contacts us requesting we change the way we are processing their personal data, we must consider their **rights** under Data Protection law.
13. You must follow system user **guidance** or other formal processes which are in place to ensure that only those with a business need to access personal data are able to do so
14. You must **share** personal data with external bodies who request it only if there is a current agreement in place to do so or it is approved by the Data Protection Officer.
15. Where the content of telephone calls, emails, internet activity and video images of employees and the public is **recorded, monitored and disclosed** this must be done in compliance with the law and the regulator's Code of Practice.
16. All employees must be **trained** to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely.
17. When using '**data matching**' techniques, this must only be done for specific purposes in line with formal codes of practice, informing service users of the details, their legal rights and getting their consent where appropriate.
18. We must maintain an up to date entry in the **Public Register of Data Controllers**
19. Where personal data needs to be anonymised or pseudonymised, for example for **research purposes**, we must follow the relevant procedure

What we must not do:

20. Share any personal data held by us with an individual or organisation based in any country outside of the European Economic Area.
21. Access personal data which you have **no right to view**

General Statement

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected

Due regard been given to Equalities Act legislation

- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely in line with the Schools retention policy

- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

The GDPR is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the GDPR should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure.

Where the GDPR does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

- Photos taken for official school use may be covered by the GDPR and pupils and students should be advised why they are being taken. (Taking photographs in schools 20140226 Version: 4.1 2).

- Photos taken purely for personal use are exempt from the GDPR.

Examples

Personal use:

- A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the GDPR does not apply.

- Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the GDPR does not apply.

Official school use:

- Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the GDPR will apply.

- A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the GDPR as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used.



Media use:

- A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the GDPR.

Complaints

Complaints will be dealt with in accordance with the school's DPO S Johnson, Woodborough Woods Foundation C of E (Aided) in line with the GDRP Legislation may 2018,

Sharon Johnson - office@woodsfoundation.notts.sch.uk

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745 3

November 2018

Reviewed biannually



Appendix 1 - Lambley School Procedures for responding to subject access requests made under the GDPR

You should complete the relevant subject access request form, available to download from our website. Paper copies are available by request from school.

The response time for subject access requests, once officially received, is 1 month (**not working or school days but calendar days, irrespective of school holiday periods**). However the month will not commence until after receipt of fees or clarification of information sought

The GDPR allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure.**

Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 1 month statutory timescale.

Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

If there are concerns over the disclosure of information then additional advice should be sought.

Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints- Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Due regard been given to Equalities Act legislation