LUNT'S HEATH PRIMARY SCHOOL

DATA PROTECTION POLICY
including GDPR

Author	Andrew Williams
Approval Date	March 2018
Reviewed	Annually
First Version	March 2018
Version	1

Lunt's Heath Primary School
Safeguarding Statement

"Lunt's Heath Primary School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and visitors to share this commitment."

Lunt's Heath Primary School
Equality Statement

"Lunt's Heath Primary School promotes equal opportunities for all pupils, staff and service users. We ensure that all persons have equal access to the full range of opportunities provided by the school. We celebrate diversity and actively encourage respect for all as well as promoting fairness and justice in the education that we provide."

SCOPE

This Policy covers the School's acquisition, handling and disposal of the personal and sensitive personal data it holds on all staff, including temporary staff, agency workers, volunteers, parents and pupils. It also applies to Governors and contractors. It explains the School's general approach to data protection which is to ensure that individual's personal data and information is protected and appropriately processed and provides practical guidance which will help to ensure that the School complies with the Data Protection Act 1998 (the Act) and anticipates the General Data Protection Regulations 2018 (GDPR).

All staff are responsible for complying with this Policy.

AUTHORITY

The Governing Body will use the General Data Protection Regulations 2018 (GDPR) as the benchmark for its standard for protecting personal data used in its day-to-day operations. The regulations explicitly state that children's data requires special attention.

STATEMENT OF POLICY

The School is required to process personal data regarding staff, pupils and their parents and guardians and friends of the School relevant to its operation and shall take all reasonable steps to do so in accordance with this Policy. Processing may include obtaining, recording, holding, handling, storage, disclosing, transportation and destroying or otherwise using data. In this Policy any reference to pupils, parents, friends or staff includes current past or prospective pupils, parents, friends or staff.

AIMS AND OBJECTIVES

- To ensure that decision makers and key people in school comply with the statutory changes to the GDPR which came into force in May 2018.
- To ensure that there will be regular reviews and audits of the information we hold to ensure that we fully meet the GDPR statutory requirements.
- To document the personal data we hold, where it came from and with whom it will be shared.
- To ensure that data collection, data handling, data storage and data disposal procedures are in line with the GDPR and cover all the rights individuals have, including how personal data is deleted and destroyed.

DEFINITIONS

Personal data is:

The GDPR applies to 'personal data' meaning 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.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data is:

Any information about a person's mental or physical health or condition, their political or religious beliefs, race, ethnicity, sexual life or orientation, trade union membership, criminal offences or alleged offences and any proceedings. The GDPR refers to sensitive personal data as "special categories of personal data". The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

The School has additional obligations in connection with the use of sensitive personal data, namely at least one of the following conditions must be satisfied:

a) Explicit consent of the data subject must be obtained; oral consent is insufficient meaning written consent will be required in all cases and on all occasions
b) Necessary for carrying out the obligations under employment, social security or social protection law or a collective agreement
c) Used in connection with alumni relations provided it relates solely to this and there is no disclosure to a third party without consent
d) Data manifestly made public by the data subject
e) Various public interest situations as outlined in the General Data Protection Regulations 2018.

The data subject is:

The person the information relates to. There may be more than one data subject, such as when a record concerns an incident involving two pupils.

The Data Controller is:

Lunt's Heath Primary School is the Data Controller and is responsible for determining the purposes of its use of data - what data it gathers and how this information is used. As the Data Controller the School is responsible for complying with the Act.

The Data Protection Officer:

The School has appointed the Headteacher as its Data Protection Officer, responsible for day-to-day compliance with this Policy. He can be contacted at Lunt's Heath Primary School by telephone on 0151 423 3322 or email Head.LuntsHeath@halton.gov.uk .

ACQUIRING, USING AND DISPOSAL OF PERSONAL DATA

The School shall only process personal data for specific and legitimate purposes.

These are:

a) providing pupils and staff with a safe and secure environment including any images on CCTV. There are currently **no** cameras around the School, but should they be installed then they will carry appropriate warning signs as to their operation. They will be used for the purpose of detecting crime, ensuring personal

security and the welfare of staff and pupils and the protection of the working environment. Images will be kept no longer than 14 days to meet these objectives, however, in certain circumstances such as an on-going investigation into criminal activity certain relevant images would be kept for longer but no longer than necessary to complete any such investigation.

b) providing an education, training and pastoral care.
c) providing activities for pupils and parents – this includes school trips and activity clubs.
d) providing academic, examination and career references for pupils and staff.
e) protecting and promoting the interests and objectives of the School – this includes fundraising.
f) safeguarding and promoting the welfare of pupils.
g) monitoring staff's email communications, internet and telephone use to ensure pupils and staff are following the School's IT Acceptable Use Policy.
h) promoting the School to prospective pupils and their parents.
i) communicating with former pupils.
j) for personnel, administrative and management purposes. For example to pay staff and to monitor their performance.
k) fulfilling the School's contractual and other legal obligations.

Staff should seek advice from the Data Protection Officer before using personal data for a purpose which is different from that for which it was originally acquired. If information has been obtained in confidence for one purpose, it shall not be used for any other purpose without the Data Protection Officer's permission.

The School shall not hold unnecessary personal data, but shall hold sufficient information for the purpose for which it is required. The School shall record that information accurately and shall take reasonable steps to keep it up-to-date. This includes an individual's contact and medical details.

The School shall not transfer personal data outside the European Economic Area (EEA) without the data subject's permission unless it is satisfied that the data subject's rights under the Act will be adequately protected and the transfer has been approved by the Data Protection Officer. This applies even if the transfer is to a pupil's parents or guardians living outside the EEA.

When the School acquires personal information that will be kept as personal data, the School shall be fair to the data subject and fair to whoever provides the information (if that is someone else) in that their data will be handled and safeguarded in compliance with the Act.

Lunt's Heath Primary School shall only keep personal data for as long as is reasonably necessary and in accordance with the retention and disposal guidelines set out in the School's Document Retention Policy. Staff should not delete records containing personal data without authorisation.

Lunt's Heath Primary School will keep personal data secure and adopt technical and organisational measures to prevent unauthorised or unlawful processing of personal data.

INFORMATION AND EXPLANATION

Privacy Notice: Individuals must be told what data is collected about them, and what it is used for. This is called a privacy notice or statement.

Purpose: The privacy notice is to ensure that the School's collection and processing of personal data is done in a transparent way so it will explain who it applies to, why the information is being collected, what information will be collected how it will be acquired and processed, what it will be used for, which third parties (if any) it will be shared with, how long records will be retained for and outline the data subject's rights, including the right to complain about the processing of their data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow. Cheshire SK9 5AF, telephone 0303 123 1113 or at: https://ico.org.uk/concerns/ .

Staff are not expected to routinely provide pupils, parents and others with a privacy notice as this should have already been provided. Copies of the School's Privacy Notice for pupils and parents can be obtained from the Data Protection Officer or accessed on the School's website.

Use: Staff should inform the Data Protection Officer if they suspect that the School is using personal data in a way which might not be covered by an existing Privacy Notice. This may be the case where, for example, staff are aware that the School is collecting medical information about pupils without telling their parents what that information will be used for.

PROTECTING CONFIDENTIALITY

Disclosing personal data within the School: Personal data will only be shared on a need to know basis. Personal data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the School or their relationship to the data subject, unless they need to know it for a legitimate purpose. Examples include – personal contact details for a member of staff (e.g. their home address and telephone number, and their private mobile telephone number and e-mail address) shall not be disclosed to parents, pupils or other members of staff unless the member of staff has given their permission.

Disclosing personal data outside of the School: Sharing personal data with others is often permissible so long as doing so is fair and lawful under the Act. However, staff should always speak to the Data Protection Officer if in doubt, or if staff are being asked to share personal data in a new way.

Before sharing personal data outside the School, particularly in response to telephone requests for personal data staff must:

a) ensure permission to share – that they have the necessary consent;

b) ensure adequate security. What is adequate will depend on the nature of the data. For example, if the School is sending a child protection report to social services on a memory stick then the memory stick must be encrypted; paper information should be sent by courier or recorded delivery, First or Second Class post is not considered secure enough. School email should be secure if sending to another @halton.gov.uk address.

c) ensure that the sharing is covered in the Privacy Notice.

The School has a duty to be careful when using photographs, videos or other media as this is covered by the Act as well. Specific guidance on this is provided in the School's Acceptable Use / Code of Conduct and Safeguarding Policies on the School's website.

Information security and protecting personal data: Information security is the most important aspect of data protection compliance and most of the fines under the Act for non-compliance relate to security breaches.

The School shall do all that is reasonable to ensure that personal data is not lost or damaged, or accessed or used without proper authority, and the School will take appropriate steps to prevent these events happening. In particular:

a) paper records which include confidential information will be kept in a cabinet or office which is kept locked when unattended.
b) the School uses a range of measures to protect personal data stored on computers, including file encryption, anti-virus and security software, sufficiently robust and frequently changed user passwords, audit trails and back-up systems.
c) staff must not remove personal data from the School's premises unless it is stored in an encrypted form on a password protected computer or memory device. Further information is available from the Data Protection Officer.
d) staff must not use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.

DATA BREACHES

Definition: A data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure or access to personal data.

Reporting obligations: Any actual data breach or alleged data breach must be reported to the Data Protection Officer as soon as it is discovered, whatever time that might be, to enable its circumstances to be investigated and appropriate action taken to limit any damage and to prevent a similar occurrence.

As soon as the School becomes aware of a significant data breach as determined by the Data Protection Officer the breach must be reported to the Information Commissioner's Office (ICO) within 72 hours. Examples of breaches and their seriousness for reporting purposes are:

a) mistakenly sending an email or letter containing personal data to an incorrect recipient.
b) theft of IT equipment containing personal data.
c) failing to deal with a Subject Access Request.

If a breach is found to be sufficiently serious i.e. if not dealt with it is likely to result in a high risk to the rights and freedoms of individuals e.g. resulting in discrimination, damage to reputation, financial loss – through identity theft or otherwise – loss of confidentiality or any other significant economic or social disadvantage then not only does this breach have to be reported to the ICO within 72 hours of its discovery, the individuals concerned must be notified of the breach in a timely manner as directed by the Data Protection Officer **(Article 29).**

DATA SUBJECT'S RIGHTS, INCLUDING ACCESSING ANY DATA HELD ON THEM

Individuals are entitled to know whether the School is holding any personal data which relates to them, what that information is, the source of the information, how the School uses it and who it has been disclosed to. This is known as a Subject Access Request.

Any member of staff wishing to exercise the right to request information covered by this policy, can do so by submitting a request in writing to the Data Protection Officer.

Any member of staff who receives a request for information covered by this policy from a pupil, parent or any other individual must inform the Data Protection Officer as soon as is reasonably possible, normally on the same day. This is important as there is a statutory procedure and timetable which the School must follow. Information must be provided to the requestor without delay and at the latest within one month of receipt.

Individuals have a right to ask the School not to use their personal data for direct marketing purposes or in ways which are likely to cause substantial damage or distress.

Individuals have a right to ask for incorrect personal data to be corrected or annotated.

Individuals have the right to object to any of their personal data being processed and to have this data erased.

Individuals have the right to restrict (halt) the processing of their personal data, usually whilst incorrect data is being corrected.

Individuals have the right to request their personal data is transferred to another data controller in a commonly used format.

Individuals have a right to ask the School not to make automatic decisions (using personal data) if such automatic decisions would affect them to a significant degree.

Individuals have the right to complain about the processing of their personal data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, Telephone 0303 123 1113 or at: https://ico.org.uk/concerns/.

DATA PROCESSORS

Where the school uses data processors (third parties / organisations that process (deals with or stores) personal data on the school's behalf, the GDPR makes written contracts between the school and the processor a general requirement and that the contract must include certain specific terms as a minimum. If the data processor then (with the school's written authority) employs another processor, it also needs to have a written contract in place.

The school will check all existing contracts and if they do not contain all the requirements it will get new contracts drafted and signed as required.

The school will ensure data processors are communicated with so they understand:

- the reasons for the changes;
- the new obligations that GDPR put on them; and
- that they may be subject to administrative fines or other sanctions if they do not comply with new obligations.

FURTHER INFORMATION

The School has registered its use of personal data with the Information Commissioner's Office and further details of the Personal Data it holds, and how it is used, can be found in the School's register entry on the Information Commissioner's website at www.ico.gov.uk under registration number Z7492448. This website also contains further information about data protection.

BREACH OF THIS POLICY

A member of staff who deliberately or recklessly discloses personal data held by the School without proper authority is guilty of a criminal offence and gross misconduct.

This could result in summary dismissal.

STATUS

This policy is intended only as a statement of School policy. It does not form part of the contract of employment and may be amended from time to time.

SUPPORTING DOCUMENTATION

- The Data Protection Act 1998
- Guide to GDPR 2018, ICO
- In the picture: A data protection code of practice for surveillance cameras and personal information 2017, ICO
- Growing Up Digital: A report of the Growing Up Digital Taskforce, Children's Commissioner 2017
- Conducting Privacy Impact Assessments Code of Practice 2014, ICO
- Subject Access Code of Practice 2017, ICO
- Education for a Connected World, UK Council for Child Internet Safety
- UN Convention on Rights of the Child
- Internet Safety Strategy Green Paper 2017, HM Government
- Code of Conduct
- Discipline Policy
- IT Acceptable Use Policy
- Privacy Notice for Staff
- Privacy Notice for Pupils and Parents
- Document Retention Policy
- Safeguarding Policy

Signed (Headteacher): Date:

Signed (Chair of Governors): Date:

APPENDIX 1 – DEFINITIONS OF DATA

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data and "sensitive" 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.

Sensitive 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;
- Criminal proceedings or convictions.

APPENDIX 2 – THE SIX PRINCIPLES

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. Processed fairly, lawfully and in a transparent manner
2. Used for specified, explicit and legitimate purposes
3. Used in a way that is adequate, relevant and limited
4. Accurate and kept up to date
5. Kept no longer than is necessary
6. Processed in a manner that ensures appropriate security of the data

APPENDIX 3

Rights of access to information

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to Mr A. Williams, Headteacher If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school will normally make no charge for the provision of information, however in cases where the request is excessive (in excess of £10), a charge will be made.

5. The response time for subject access requests, once officially received, is 28 days **(not working or school days but calendar days, irrespective of school holiday periods)**. However the 28 days will not commence until after receipt of fees or clarification of information sought.

6. The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

7. 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 40 day statutory timescale.

8. 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.

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

10. 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.

11. 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.

12. 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.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact Mr A. Williams, Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone