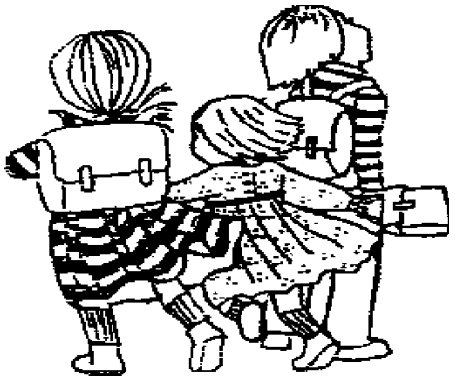
Long Marton School

Data Protection Policy



May 2018

Introduction

The Governing Body of Long Marton school recognises its responsibilities under the General Data Protection Regulations (GDPR) as a Data Controller, ensuring policies, procedures and safeguards are in place to comply with the data protection principals and associated requirements.

This policy is intended to ensure that personal data is dealt with correctly and securely and in accordance with the (GDPR), 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.

Data Protection Principles

The GDPR principals set out the main responsibilities for organisations. Article 5 of GDPR requires that personal data shall be:-

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

In addition, Article 5 (2) requires that "the controller (i.e. the school) shall be responsible for, and be able to demonstrate, compliance with the principals".

Accountability and Governance

To ensure that the school discharges its responsibilities in accordance with the above principals and personal information is handled in a safe and secure manner and in a culture of transparency, the school will:

- Promulgate appropriate policies and procedures, and data retention schedule including data minimisation where appropriate.
-
- Ensure all staff, volunteers and governors are aware of their responsibilities under GDPR and the schools policies and procedures regarding the collection, processing and disclosure of personal data and relevant documentation and receive appropriate training.

- Implement appropriate technical and organisational measures that ensure and demonstrate it complies with the requirements of GDPR. This will include relevant policies and procedures, staff, governor and volunteers training and induction processes, audits of processing activities and security safeguards.

- Maintain documentation on processing activities, including the information required under Article 30 of GDPR, records of consent other relevant documents.

- Where Consent is the lawful basis for processing, the data subject(s) must actively opt-in (in words, not by tick box). In addition, they must be informed why the data is required, what the school will do with it, name of any third party controllers who will reply on the consent, and that they can withdraw consent at any time.

- Records demonstrating consent must be kept. The required information will be included on the school's data controller spreadsheet with links enabled to other relevant documents. The spreadsheet will be posted on the links page of the school website in read only mode.

- Regularly test, assess and evaluate the effectiveness of its security measures, documenting the results and acting upon any recommendations which arise.

- Ensure that third parties with whom the school have contracts, servicer agreements and commercial engagement are GDPR compliant.

- Appoint a Data Protection Officer (DPO) whose tasks will include:-

    Informing and advising the governing body, staff and volunteers about their obligations to comply with the GDPR and other data protection laws.

    Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; ensure governors, staff and volunteers receive appropriate training and conduct internal audits.

    The first point of contact for supervisory authorities and for individuals whose data is processed.

In accordance with legal requirements, the DPO operates independently without fear of dismissal or penalty for performing their tasks, will report directly to the school's full governing body, and be provided with adequate resources to meet their obligations.

The DPO appointed for Long Marton school is Peter Brown.

In making the appointment, due consideration has been given to ensuring no conflict of interest will arise due to any other role undertaken by the individual appointed, their level of expertise and knowledge required being proportionate to the type of processing undertaken by the school and the level of protection the personal data requires.

Definition of "Personal Data"

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.
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.

Special categories of personal data

This is data which is more sensitive, and so needs more protection. For example, any of the following information about an individual:

race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, sexual orientation.

Within the context of this school, such special categories could include:-

- Staff Trade Union details;
- Information on the racial or ethnic origin of a child or member of staff to comply with its public sector duty under the Equality Act 2010;
- Information about the sexuality of a child, or their family or a member of staff to comply with its public sector duty under the Equality Act 2010;
- Medical information about a child or member of staff;

On some occasions it is important that medical information should be shared more widely to protect a child - for instance if a child had a nut allergy how it should be treated. Where appropriate, written permission should be sought from the parents/carers before posting information more widely, for instance in the staff room.

Personal data processed by the school

The school has access to a wide range of personal information and data, most of which is processed due to statutory or contractual requirements. This includes:-

- Personal information about members of the school community – including pupils, members of staff, parents/carers, governors and volunteers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records.

- Curricular/academic data e.g. class lists, pupil / student progress records, reports, references.

- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references.

- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

In determining whether the data should be processed, the school has considered whether it is proportionate and necessary for the stated purpose rather than the chosen method of pursuing that purpose.

Data Protection Impact Assessments (DPIA)

The school will undertake Data Protection Impact Assessments when using new technology or the processing is likely to result in high risk to the rights and freedoms of individuals;

The information contained within the DPIA will include:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- Assessment of the necessity and proportionality of the processing in relation to its purpose.
- Assessment of the risks to individuals.
- Measures in place to address risk, including security and to demonstrate compliance

Privacy Notices (the 'right to be informed')

The school publishes information about how it processes personal data in the form of Privacy Notices. These notices will be provided free of charge to individuals whose personal data the school process and, in the case of pupils, to parents/carers through a letter. The notices are also posted on the links page of the school's website. The information which must be provided in the privacy notices is shown below.

	Data obtained directly from data subject	Data not obtained directly from data subject
What information must be supplied	**Not required when the data subject has the information**	**Not required when data subject has the information**
Name & contact details of school and the DPO	Yes	Yes
Purpose of the processing and the legal basis for it	Yes	Yes
Where appropriate, the legitimate interests of the school or third party	Yes	Yes
Categories of personal data		Yes
Details of transfers to third country and safeguards	Yes	Yes
Retention period or criteria used to determine retention period	Yes	Yes
Existence of each data subject's rights	Yes	Yes
Where relevant, the right to withdraw consent at any time	Yes	Yes
The right to lodge a complaint with a supervisory authority	Yes	Yes
The source the personal data originates from and whether it came from publically accessible sources		Yes
Whether provision of the data is part of statutory or contractual requirements or obligation; and possible consequences of failing to provide data	Yes	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	Yes	Yes

When the information should be provided	**Data obtained directly from data subject**	At the time the data are obtained
	Data NOT obtained directly from the data subject	Within a reasonable period of obtaining it (within one month) If the data are used to communicate with the subject, at the latest, when the first communication takes place; or If disclosure to another recipient is envisaged, at the latest before the data are disclosed

Personal data breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party (for example, data seen by visitor, insecure disposal of paper records);
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient (for example, emails);
- computing devices containing personal data being lost or stolen (for example, tablets, USB sticks);
- alteration of personal data without permission;

- loss of availability of personal data (for example, cyberware attack, backup procedures not followed).

In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

In the event of a personal data breach:

- the DPO will establish the likelihood and severity of the resulting risk to people's rights and freedoms.
- If it is likely that there will be a risk the DPO will notify the ICO within 72 hours and the individuals concerned without undue delay;
- if it's unlikely, there is no need to report it;
- in either case, the cause of the breach should be investigated and documented with a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects, including, if relevant, the justification for not reporting the matter to the ICO.

Responsibilities regarding obtaining, recording and disclosing personal data

The school and any individuals collecting, processing and disclosing data must:

- Only obtain personal data from those sources specified in the privacy notice(s).
- Use the data only for the purpose(s) for which it is obtained as specified in the privacy notices
- Satisfy themselves that the data is accurate and recorded accurately.
- Take steps to ensure that data that is inaccurate is erased or rectified without delay.
- Disclose the data (either intentionally or accidentally) only to someone to whom disclosure is authorised or in accordance with the privacy notice(s)
- Satisfy themselves as to the identity of the person to whom the disclosure is made
- Take care not to disclose data unintentionally through casual conversation or use of social media sites
- Kept in a form which permits identification of the subject for no longer than necessary for the purpose for which it is processed

Security of Personal Data

GDPR requires that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Regulations also state that the nature, scope, context and purpose of processing should be taken into account in implementing the measures to ensure a level of security appropriate to the risk.

An analysis of the risks in accordance with the above criteria has been made and the measures as detailed below put in place.

Notwithstanding such measures, it is emphasised that everyone who accesses or uses personal data processed by the school has a part to play in keeping it safe from loss and unlawful disclosure.

Organisational measures/working practices

- Access to and within, the school by non-school staff will be in accordance with the Security and Visitor policy.

- Documents should be proactively marked to protect personal data more effectively using the Government's security classifications. Within the school environment, those marking are:

Type of Data	Marking
Public This would include any information not containing any personal data, or information in the public domain. This includes :- *Lesson Plans and Teaching resources* *Public Documents such as policies etc.*	***Public Domain*** ***or*** ***not Protectively marked***
Official – Personal This category should be used for all personal data, which is not defined as sensitive e.g. Contact Details of Parents, Assessment information etc.	***Official***
Official – Sensitive This category would include any data deemed to be "Sensitive Personal Data" and access to this should only be on a "Need to Know" basis. Additional security measures may be needed for data in this category.	***OFFICIAL – SENSITIVE***

- Documents containing personal data should only be printed where absolutely necessary and only in sufficient copies for the purpose required. Where documents are printed, care should be taken to ensure all copies are collected from the tray. If a document or part of it has not been printed, the print should be cancelled.

- All paper based personal data will be protected by appropriate controls, for example:

  - Paper based safeguarding chronologies will be in a locked cupboard when not in use;

  - Class Lists used for the purpose of marking may be stored in a teacher's bag;

  - Paper based personal information sent to parents will be checked by, Headteacher, School Business Manager or SENCO before the envelope is sealed.

- Personal data in paper form will be kept in locked cabinets/receptacles. Where documents are removed from the site of storage, the date of removal will be logged together with the purpose, identity of the individual concerned and the subsequent return date.

- Documents/printouts containing personal data should not be left unattended where they could be read, either deliberately or accidentally, by someone not authorised to see them. Where they are removed from the school site for out of school activities they should be kept in a secure bags/receptacles.

- Governors should ensure that any printed material from school or printed at home containing personal data should be kept secure, not shared with an unauthorised person, and destroyed when its retention is no longer relevant by shredding or burning.

- When copies of documents and print of emails containing personal data are no longer required for the purpose for which they were printed, they should be destroyed as soon as practicable either by shredding or burning.

- The back-up procedures for data held on school systems should be carried out in accordance with the Business Continuity Plan. In the event of an emergency situation requiring the school to be vacated, where safe and practicable, IT equipment and paper documents should be recovered from the school in line with the Disaster Recovery Plan.

- All storage media and backup data, including off-site backups, must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

- When a request is made for information or documents containing personal data, the identity of the caller must be confirmed.

Technical measures

- Personal data should only be stored on school equipment. This includes computers and portable storage media (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data without express consent of the DPO who must be satisfied that security of the personal data will not be compromised.

- School computers should be protected by suitable firewalls and anti-virus software, and necessary security updates. Data from portable devices should not be downloaded without scanning

- Access to personal data on school computers will be protected with strong passwords which are changed at least termly and when it is believed they have been compromised, Members of staff will not, as a matter of course, be granted access to the whole management information system and will be assigned clearance which determines which files are accessible according to their roles and responsibilities.

- When unattended, even for very short periods, computers will be set to auto lock if not used for a period of time.

- Staff, governors and volunteers will be allocated email addresses by the school for the exchange of material containing personal data. Emails from school will contain a signature block requiring confirmation that it has been received by the correct recipient or otherwise.

- Personal data will be transmitted by attaching the material in which it is included as a word document and encrypting the document/compressing with 7 zip and encrypting. The recipient will then need to contact the school for access to a one-off password. If downloaded onto home computers.

- Export of personal data from the school's computer files onto mobile devices will be logged with details of the individual, the reason, the length of time they will keep the data
  .
- Portable computer systems and mobile devices on which personal data is stored should be protected by password or biometric authentication.

- Only encrypted USB sticks purchased by the school will be used to store personal data. The data must be securely deleted from the device once it has been transferred or its use is complete.

- Images of pupils will be stored in a secure area and only transferred and transported by use of protected or encrypted devices

- The school will ensure that any supplier used for cloud based storage confirms that it fully meets the issues identified in the Department of Education self-certification checklist and is compliant with the obligations under GDPR. The school should also assess the level of risk of disruption due to the loss of network connectivity, and adopt reasonable measures to cope with that risk.

- Uploads to the school website will be checked prior to publication to ensure that appropriate photographic consent has been obtained and that the correct documents have been uploaded.

Right to Rectification.

GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.

Briefly:

- A request for rectification may be made verbally or in writing,
- the school must respond within one calendar month;
- In certain circumstances a request for rectification can be refused.

Please refer to the ICO Guide to the General Data Protection Regulations (GDPR) for further guidance on that or other matters relating to GDPR:-

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Complaints

Any individual who believes that their personal data has been compromised may complain to the DPO. If they are not satisfied with the manner in which their complaint was handled, the reason for the decision should be explained, and they should be informed of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

Right of Access (subject access)

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data;
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

Proof of Identity:

The identity of the person making the request should be verified using 'reasonable means', and, where necessary a check carried out regarding proof of relationship to the child.

Fees for subject access requests:

A copy of the information must be provided **free of charge**; however, a 'reasonable fee' may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive;

A reasonable fee may also be charged to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests;

Fees must be based on the administrative cost of providing the information.

Timescale for response:

Information must be provided without delay and at the latest within **one calendar month** of receipt.

The period of compliance may be extended by a further two months where requests are complex or numerous. If this is the case, the individual must be informed within one month of the receipt of the request why the extension is necessary.

Manifestly unfounded or excessive requests:

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can: charge a reasonable fee taking into account the administrative costs of providing the information; or refuse to respond.

Requests for large amounts of personal data:

Where you process a large quantity of information about an individual, the GDPR permits you to ask the individual to specify the information the request relates to (Recital 63).

The GDPR does not include an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

Third party and pupil data

Before disclosing third party information consent should be obtained. Third party information is that which has been provided by another (e.g. Police, Health Care professional, Local Authority, or another school; however, there is still a need to adhere to the 40 day 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, additional advice should be sought.

Manner of disclosure:

Where redaction has taken place, 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, and codes or technical terms clarified and explained. If information contained within the disclosure is difficult to read or illegible, it should be retyped.

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. 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.

If the request is made electronically, you should provide the information in a commonly used electronic format.

See also:

Privacy notice

Data Controllers Spreadsheet

Governors' Code of Conduct

Security and Visitor policy

Whistleblowing policy

Date: 2nd May 2018 Review: May 2020

Signed:

Chair of Governors