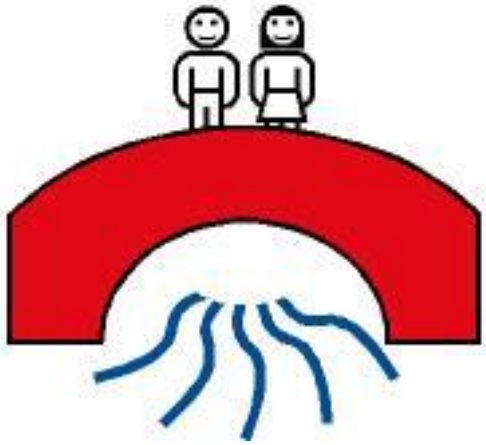
Loddon Primary School



General Data Protection Regulations (GDPR) Policy

Author: Wokingham Borough Council

Committee responsible: Full Governing Body

Date of last review: n/a

Date of next review: May 2019

Authorised on 23 May 2018

.....	Sarah Phillips	Headteacher
.....	Rob Henderson	Chair of Governors

Data Protection Policy template v1.1
(updated for GDPR/Data Protection Act 2018)

1. Introduction
    a. Our school is committed to protecting all data that it holds relating to staff, pupils, parents and governors.
    b. This policy applies to all school data including CCTV, please refer to our CCTV Policy), regardless of whether it is in paper or electronic format and where it is stored.
    c. This policy was approved by governors on 23 May 2018 and will be reviewed annually.

2. Legislation and guidance
    a. This policy meets the requirements of the Data Protection Act 2018 [law from 25 May 2018] (which incorporates the General Data Protection Regulation) and is based on guidance published by the Information Commissioner's Office (ICO) and the Department for Education. All staff and governors should note that the Act makes provision for significant fines to be levied in the event of non-compliance.
    b. Section 6 also refers to the Education (Pupil Information) (England) Regulations 2005.
    c. Section 7 refers to the Freedom of Information Act 2000.

3. Data protection principles and categories of data
    a. The Data Protection Act 2018 [law from 25 May 2018] sets out six data protection principles that the school must follow when processing personal data. Data must be:
        - Processed fairly, lawfully and in a transparent manner
        - Used for specified, explicit and legitimate purposes
        - Used in a way that is adequate, relevant and limited
        - Accurate and kept up-to-date
        - Kept no longer than is necessary
        - Processed in a manner that ensures appropriate security of the data

    b. Categories of data
        i. The Data Protection Act 2018 [law from 25 May 2018] refers to **Personal data** and **Special categories 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.
            - **Special categories of personal data** (previously known as 'sensitive personal data') includes race, ethnic origin, politics, religion, trade union membership, biometrics, health and sexual orientation.
        ii. Note that the DfE consider it best practice that data such as free school meal status, pupil premium eligibility, elements of special educational need information, safeguarding information, some behaviour data and Children's Services interactions are also treated with the same care as the special categories set out in law.

4. Roles and responsibilities

a. The Data Controller
    i. Our school processes personal information relating to pupils, staff and visitors (defined as 'Data Subjects') and is therefore a Data Controller.
    ii. The governing body has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 2018 [law from 25 May 2018].
    iii. The Headteacher will ensure the provisions of this policy are in place and that all staff are aware of their data protection obligations.
    iv. Day to day responsibility for Data Protection will reside with the Data Protection Officer (DPO).
    v. The school is registered as a Data Controller with the ICO and renews this registration annually.
b. Data Protection Officer (School Business Manager)
    i. The Data Protection Officer will:
        - Act as the contact point for all Data Protection issues and queries from Data Subjects and the ICO, e.g. for Subject Access Requests, data breaches, following the agreed procedures (see Appendix).
        - Maintain appropriate documentation related to data processing.
        - Undertake the training necessary to fulfil their role, and ensure staff have access to appropriate training and updates.
        - Monitor compliance with all aspects of Data Protection.
        - Provide advice relating to Data Protection Impact Assessments (DPIA) e.g. before introducing a new data processing system.
        - Annually review the ICO licence.
c. School staff
    i. All school staff, in whatever role, have a duty to comply with this policy. Failure to comply may result in disciplinary action.
    ii. Staff must report any data related concerns or breaches immediately to the DPO.
d. Data processor
    i. The school uses a range of third parties to process data on our behalf, e.g. payroll, catering, communications. The school will ensure that all data processors are compliant with the Data Protection Act 2018 and that contracts include obligates on the data protection in compliance with GDPR
e. Sharing data
    i. Where data is routinely shared with other organisations (e.g. Local Authority, DfE, NHS, Police) the school will ensure this is made clear in the Privacy Notice and that appropriate protocols are in place.

5. Data Protection documentation
    a. Privacy Notices
        i. The school will make available Privacy Notices for Pupils/Parents, Staff and Governors that set out how the school will make use of their personal data. These will be made available via the school website.
    b. Consent
        i. Where required the school will seek and record specific consent from data subjects (e.g. image permissions, email marketing, biometrics).
    c. Data Protection Audit/record keeping/logs

i. The school will maintain suitable records which detail all data that is collected, processed and where appropriate shared. The Key audit tool will be used for this purpose. In addition, the school will keep records of other key areas including:
   - Subject Access Requests – see Appendix (b)
   - Data Breaches – see Appendix (a)
   - Data retention schedule, disposal/destruction log using the Information and Records Management Society (IRMS) Toolkit for Schools (copy in office manual)
   - DPIA
   - Requests for changes to data
   - A general description of the technical and organisational security measures that are in place

6. Subject Access Requests/Parental requests to see the educational record
   a. Under the Data Protection Act, pupils (or their parents for children under 13) have a right to request access to information the school holds about them. This is known as a Subject Access Request (SAR).
   b. The SAR process and timescales are provided in Appendix (b).
   c. In addition, maintained schools, PRUs and non-maintained special schools should be aware of Regulation 5 of the Education (Pupil Information) (England) Regulations 2005 that gives parents the right of access to their child's educational record, free of charge, within 15 school days of a request.
   d. The Education (Pupil Information) Regulations noted above do not apply to non-maintained schools, such as academies. Parents of children at non-maintained schools wishing to access information must therefore make a SAR.

7. Freedom of Information Act (FOI)
   a. The school will comply with the Freedom of Information Act 2000.
   b. All FOI requests will be directed to the DPO who will follow the procedures outlined in the Appendix (c).
   c. The school will comply with the requirement to produce a publication scheme following the guidance available from the ICO.

8. Security and storage
   a. The school will ensure that appropriate technical and organisational measures are in place to protect school data.
   b. The school will ensure that staff and governors are only able to access data that is relevant to their role.
   c. The school will ensure that staff and governors are provided with specific guidance, which should include for example:
      - Use of encrypted USB flash drives/memory sticks and other removable media
      - Appropriate use of professional and personal email accounts
      - Use of encrypted/Secure email
      - Secure storage of paper files, clear desk policies, etc
      - Screen locking procedures when not working at your desk
      - Use of cloud based storage
      - Taking data off site/Home working

- Use of staff personal devices
- Passwords
- Encryption of school devices that may be taken off site, e.g. staff laptops.

d. Key points from the list above will be included in Staff Acceptable Use Agreements.

9. Retention and disposal
    a. The school will produce a document retention and disposal schedule. This will be based on the retention guidelines from the Information and Records Management Society (IRMS) Toolkit for Schools and any other guidance, e.g. DfE or Local Authority
    b. Appropriate measures will be taken to ensure that data that is no longer required, whether in paper or electronic form, is disposed of securely.
    c. The school will ensure appropriate disposal of all devices that hold school data.
    d. A destruction record will be kept for all data and devices that are disposed of.

10. Training
    a. All staff and governors will be provided with data protection training as part of their induction process.
    b. Data protection training, briefings and updates will also be provided for all staff and governors as required, but at least every two years.

Appendix

(a) Data breach information and procedures

Data protection breaches can be caused by a number of factors, e.g. Loss or theft of pupil, staff or governing body data and/or equipment or paperwork on which data is stored, inappropriate access controls allowing unauthorised use, poor data destruction procedures, human error such as sending an email to the wrong person, cyber-attack, hacking, ransomware.

In the event of a breach, the procedures below should be followed:

1. Any data protection incident should be reported immediately to the school's DPO (SBM) and Headteacher.
2. If required, appropriate actions should be taken to halt the breach, and/or prevent further breaches.
3. The DPO must report any significant data protection incidents to the ICO.
    - This should take place within 72 hours of the breach being detected, where feasible.
    - If in doubt as to the significance of the incident, seek external advice, which could involve contacting the ICO.
    - If some details of the breach are yet to be determined, it would be appropriate to make an initial report to the ICO, followed up by a further report once more is known.
4. The Chair of Governors should be informed as soon as possible. Other agencies as appropriate may need to be informed depending on the breach, e.g. police, Action Fraud, social services.
5. Where the breach involves the disclosure of the personal data of specific individuals, they should usually be notified within 72 hours of detection
6. Fully investigate the breach, and review all related policies and procedures to make any necessary changes.
7. Report any findings to the Senior Management Team
8. Provide additional training to staff as appropriate.
9. Review whether any disciplinary action should be taken.
10. If the nature of the breach could result in adverse publicity the school may wish to prepare a statement for publication.
11. A full record should be kept of all data breaches, including all the steps taken, whether reportable or not.

Additional notes

In the event of a data breach, the following areas will need to be considered:

- The type of data and its sensitivity
- What protections were in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

(b) Subject Access Request (SAR) process and timescales

A SAR is a request for personal data about the applicant. Where pupils are under the age of 13, a SAR will be made on their behalf by the parent/guardian. Pupils 13 and above may make a SAR in their own right. Where a parent of a pupil 13 and above makes a SAR, it should be with the agreement of the pupil.

All SARs must be in writing, either paper or electronic, and should be directed to the DPO who will follow the procedure outlined below:

1. Clarify that this is a SAR and not some other request for information, i.e. a FOI request or an 'educational record' request.
2. Confirm the identity of the person making the request.
3. If it is unclear what information is being requested, ask for further details from the applicant.
4. Check that the information is available:
    - If the information is not available, inform the applicant.
    - If the information is available, note the date that the SAR was received or, in the case of further details being requested, the date that these were received. The school now has one calendar month to respond.
5. Check whether the information requested contains information about any third-party. If it does then undertake one, or more, of the following steps:
    - Seek permission to disclose the information from the third-party concerned.
    - Redact/summarise the information to protect the identity of the third-party.
    - Withhold the information to protect the rights of the third-party.
6. Ensure that the information to be supplied is clear and understandable, e.g. any complex codes or terms are explained.
7. Supply the information requested in an appropriate format, e.g. if the request is made electronically, the information should be provided in an electronic format.
8. Keep a record of the SAR and any information that was supplied.

Additional notes

- The school must provide a copy of the information free of charge. However, schools can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The school may also charge a reasonable fee to comply with requests for further copies of the same information. The fee must be based on the administrative cost of providing the information.
- The school will be able to extend the one month period of compliance by a further two months where requests are complex or numerous. If this is the case, the school must inform the applicant within one month of the receipt of the request and explain why the extension is necessary.
- The school might also decide to withhold some information. Examples of some information which (depending on the circumstances) it might be appropriate to withhold include:
    - information that might cause serious harm to the physical or mental health of the pupil or another individual;
    - information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
    - information contained in adoption and parental order records; and
    - certain information given to a court in proceedings concerning the child.
- More information about SARs is available on the ICO website.

(c) Freedom of Information (FOI) process and timescales

The school has a publication scheme, which outlines the information that is routinely made available. This can be found on the school website.

A FOI request may be made by any member of the general public, as they have a right to know about the activities of public authorities, which includes schools. The school will normally disclose the information requested in whole or part unless there is a clear and accepted reason not to do so.

All FOI requests must be in writing, either paper or electronic, and must contain the applicant's contact details. All requests should be directed to the DPO who will follow the procedure outlined below:

1. Clarify that this is a FOI request and not some other request for information, i.e. a SAR or an 'educational record' request.
2. If it is unclear what information is being requested, ask for further details from the applicant.
3. Check that the information is available:
    - If the information is not available, inform the applicant.
    - If the information is available, note the date that the FOI request was received or, in the case of further details being requested, the date that these were received. The school now has 20 school days to respond.
4. Check whether there is any good reason for refusing to disclose part or all of the information requested. Seek guidance from the ICO if in any doubt.
5. Ensure that the information to be supplied is clear and understandable.
6. Supply the information requested in an appropriate format, e.g. if the request is made electronically, the information should be provided in an electronic format.
7. Keep a record of the FOI request and any information that was supplied.

Additional notes

- The school may charge for the cost of copying and postage, where appropriate.
- The school may refuse an entire request under various circumstances, e.g.:
    - It would cost too much or take too much staff time to deal with the request (although note that the ICO guidance relating to this aspect indicates that the work required would have to be very substantial before a refusal would be acceptable).
    - Where complying might prejudice someone's commercial interests. However, it has to pass the 'Public Interest Test', i.e. that on balance the public interest in withholding the information outweighs the public interest in disclosing it.
    - The request is vexatious.
    - The request repeats a previous request from the same person.
- Further advice on when a FOI request may be refused is available from the ICO.