Orchard Lea Federation Data Protection Policy

Date agreed: May 2023

Date for renewal: May 2024

The school collects and uses personal information (referred to in the General Data Protection Regulation (GDPR) as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The school is the Data Controller, of the personal data that it collects and receives.

The Admin Officer is the Data Protection Officer, who may be contacted through the school office. Our contact details are on our website.

The school issues Privacy Notices (also known as a Fair Processing Notices) to all pupils/parents and staff on entry to the school. These summarise the personal information held about pupils and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data.

Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information/ data?

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles

The GDPR establishes principles as well as a number of additional duties that at Orchard Lea we know must be must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner.

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes).

3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive.

4. Personal data shall be accurate and where necessary, kept up to date.

5. Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6. Personal data shall be processed in a manner that ensures appropriate security of the personal.

7. The controller shall be responsible for and be able to demonstrate compliance with the UK GDPR.

Duties

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

Commitment

At Orchard Lea we are committed to maintaining the principles and duties relating to GDPR at all times. Therefore, we will:

- Inform individuals of the identity and contact details of the data controller on our website and when pupils/staff first join the school.
- Inform individuals of the contact details of the Data Protection Officer on our website and when pupils/staff first join the school.

- Inform individuals of the purposes that personal information is being collected and the basis for this. For example, through our Privacy Notice.
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this. For example, the school may contact a parent if they need to refer a child to an outside agency for further support.
- If the school plans to transfer personal data outside the EEA, the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information.
- Inform individuals of their data subject rights.
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept through a link to our retention policy.
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent.
- Check the accuracy of the information it holds and review it at regular intervals. We will ask parents to update us with new information at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in. We will keep information in a secure place and ensure that all staff have training on the importance of keeping information safe.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed through following our retention schedule.

- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests)
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards.
- Ensure that all staff and governors are aware of and understand these policies and procedures.

Use of Biometric Data

At Orchard Lea we understand that the term 'biometric data' means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.
We do not collect or store any biometric data regarding staff or pupils and are aware of the guidance in the DFE publication, *Protection of biometric information of children in schools and colleges, Advice for proprietors, governing bodies, head teachers, principals and school and college staff. March 2018.*

Breach of GDPR

Anyone who does not adhere to the principles of GDPR must report the breach to the Executive Headteacher immediately, noting detail on the form in appendix 1. The aim of this document is to ensure that, in the event of a security incident such as personal data loss, information can be gathered quickly to document the incident, its impact and actions to be taken to reduce any risk of harm to the individuals affected. The details will reviewed by the Data Protection Officer who will determine the implications for the school, assess whether changes are required to existing processes and notify the ICO / data subject where appropriate. Breaches will be reported to the ICO within 72hours.

Training

All staff will receive training about the principles behind GDPR on induction into the school. Training will be refreshed through reminders on weekly briefings and annually in staff meetings at the beginning of each Autumn term.

Subject Access Requests

Members of the school community are able to make a subject access request to find out what information the school holds and how the information is used. Whilst a request can be made verbally, we would ask that requests are made in writing clearly outlining the reasons for the request and how information is to be sent out. The request can be made through the school office.The school will then comply with the request within one month.

Complaints

Should any member of the school community feel that the school has not adhered to the principles of GDPR, then complaints will be dealt with in accordance with the school's complaints policy. The first step is to inform the Executive Headteacher of the complaint. Our complaints policy can be found on our website and details the next steps. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Contacts

If you have any enquires in relation to this policy, please contact the school office who will also act as the contact point.

Appendix 1

DATA BREACH REPORTING FORM

The aim of this document is to ensure that, in the event of a security incident such as personal data loss, information can be gathered quickly to document the incident, its impact and actions to be taken to reduce any risk of harm to the individuals affected.

The checklist can be completed by anyone with knowledge of the incident. It will need to be submitted and reviewed by the Data Protection Officer who can determine the implications for the school, assess whether changes are required to existing processes and notify the ICO / data subject where appropriate.

SUMMARY OF INCIDENT	
Data and time of incident	
Nature of breach (e.g. theft/ disclosed in error/ technical problems)	
Give a full description of how breach occurred	
PERSONAL DATA	
Give a full description of all the types of personal data involved with the breach but not specifically identifying the individual concerned (e.g. name, addresses, health information etc.)	
How many individuals are affected?	
Have the affected individuals been informed of the incident?	
Is there any evidence that the personal data involved in this incident has been further disclosed? If so, please provide details	

IMPACT OF INCIDENT	
What harm is foreseen to the individuals affected? (e.g. could the breach increase the risk of identity theft?)	
What measures have been taken to minimise the impact of the incident?	
Has the data been retrieved or deleted? If yes, state when and how	
REPORTING	
Who became aware of the breach?	
How did they become aware of the breach?	
Form Completed by	
Position	
Date	