Oakleigh School
& The Early Years Centre

General Data Protection Regulation Policy

Rationale & Purposes

Guidelines

1. Legal framework
2. Applicable data
3. Principles
4. Accountability
5. Data protection officer (DPO)
6. Lawful processing
7. Consent
8. The right to be informed
9. The right of access
10. The right to rectification
11. The right to erasure
12. The right to restrict processing
13. The right to data portability
14. The right to object
15. Privacy by design and privacy impact assessments
16. Data breaches
17. Data security
18. Sharing Information
19. Publication of information
20. Photography
21. Data retention
22. DBS data
23. Policy review

Rationale

Oakleigh School and EY Centre is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the GDPR.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

Purposes

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the GDPR.

Organisational methods for keeping data secure are imperative, and **Oakleigh School and EYC** believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

Guidelines

1. Legal framework

1.1. This policy has due regard to legislation, including:

- The GDPR
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

1.2. This policy will also have regard to guidance from the Information Commissioner's Office:

1.3. This policy will be implemented in conjunction with the following other school policies:

- **Internet Safety & Appropriate Use Policy – due to be ratified**
- **Critical Incident Plan – covers loss of school records**
- **Child Protection policy**. Information relating to children is now entered on the secure Tootoot platform. Referrals to the social care team will be made using the secure Multiagency Safeguarding Hub
- **H&S Policy Appendix 6 - Equipment Safety incl. Laptop Loan policy**

2. Data

2.1. **Personal dat**a includes any combination of data items that identifies an individual incl. certain combinations of information, e.g. names and addresses or DoB, first name & surname, or photos and first names or unique pupil numbers.

2.2. Sensitive data includes data about racial or ethnic origin, allegations of an offence biometric data (fingerprints etc.) and data concerning health matters.

3. Principles

3.1. Personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes.
- Relevant and limited to what is necessary for these purposes.
- Accurate and updated where necessary
- Kept only as long as necessary, except for anonymised data such as that used for government statistics.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised processing and against accidental loss, using appropriate technical or organisational measures. Personal data should be put out of sight overnight, unless this interferes with the smooth running of the class, or if away from the desk for a long period.

3.2. The GDPR also requires the headteacher, as the data controller, to 'be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1. **Oakleigh & EYC** will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

4.2. The school will have comprehensive, clear and transparent data protection processes.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

4.4. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules (usually 5 years from leaving the school for staff, 25 years or longer for pupils, though these may cross over to secondary school)
- Categories of recipients of personal data
- Description of technical and organisational security measures

- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4.5. The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Anonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously improving security features.

4.6. Risk assessments will be made around data processing procedures. Data protection impact assessments will be used, where appropriate.

5. Data protection officer (DPO)

5.1. A DPO, which can be an external body, a single member of school staff or a group of staff and governors will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2. An existing employee can have or share the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests. There will generally be more than one person with responsibility for data protection procedures in case of conflict of interests.

5.3. The individual appointed as DPO will need to gain experience and knowledge of data protection law and procedures, particularly that in relation to schools.

5.4. The DPO will report to the highest level of management at the school, which is the **headteacher**.

5.5. The DPO will operate independently and will not be dismissed or penalised for performing their task.

5.6. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. The school will act as a data processor; however, this role may also be undertaken by other third parties, in which case, the school will take due diligence to see that those third parties are compliant with GDPR.

6.3. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - Compliance with a legal obligation.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - For the performance of a contract with the data subject or to take steps to enter into a contract.
  - Protecting the vital interests of a data subject or another person.
  - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

6.4. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body such as the local authority or the government, provided there is no disclosure to a third party without consent.
- Processing relates to personal data clearly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.

- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of the law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of the law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

7. Consent

7.1. Consent will be sought prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement.

7.2. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.3. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.4. Where consent is given, a record will be kept documenting how and when consent was given.

7.5. The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.6. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR, but does not need to be reobtained.

7.7. Consent can be withdrawn by the individual at any time.

7.8. The consent of parents/carers will be sought prior to the processing of their children's data.

8. The right to be informed

8.1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

8.2. In relation to data obtained, the following information will be supplied within the privacy notice:

- The contact details of the controller (the school), as well as the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time.
  - Lodge a complaint with a supervisory authority.

8.3. Information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

8.4. Information regarding the categories of personal data that the school holds, and the source that the personal data originates from will be provided.

9. The right of access

9.1. Individuals have the right to obtain confirmation that their data is being processed.

9.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

9.3. The school will verify the identity of the person making the request before any information is supplied.

9.4. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

9.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

9.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

9.7. All fees will be based on the administrative cost of providing the information.

9.8. All requests will be responded to without delay and at the latest, within one month of receipt.

9.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.10. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.11. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

10. The right to rectification

10.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

10.2. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

10.3. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5. Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to erasure

11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation

11.3. The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

11.4. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11.5. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. The right to restrict processing

12.1. Individuals have the right to block or suppress the school's processing of personal data.

12.2. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

12.3. The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

12.4. If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.5. The school will inform individuals when a restriction on processing has been lifted.

13. The right to data portability

13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

13.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

13.3. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract

- When processing is carried out by automated means

13.4. Personal data will be provided in a structured, commonly used and machine-readable form.

13.5. The school will provide the information free of charge.

13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

13.8. In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

13.9. The school will respond to any requests for portability within one month.

13.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

13.11. Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. The right to object

14.1. The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

14.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

14.4. Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

14.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

15. Privacy by design and privacy impact assessments

15.1. The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

15.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

15.3. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

15.4. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

15.5. A DPIA will be used for more than one project, where necessary.

15.6. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- (The use of CCTV – not currently in use).

15.7. The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

15.8. Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

16. Data breaches

16.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

16.2. The **headteacher** will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

16.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

16.4. All notifiable breaches will be reported to the relevant supervisory authority (LA Data Protection Officer, &, where necessary the ICO) within 72 hours of the school becoming aware of it.

16.5. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

16.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

16.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

16.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

16.9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

16.10. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

16.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

17. Data security

17.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

17.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

17.3. Children's record files, registers and class lists (and other personal information which contain specific details of pupils) should not generally be on display. Such information should be readily available to staff. PLPs, can be on display on classroom walls etc., but with sensitively written targets (e.g. if they include toileting information or behaviour support). Any information stored on classroom walls or in pockets on the wall must ONLY have first name and photo. No other identifying information must be on these documents (e.g. date of birth). (First names will be used rather than full names, without DoB. in PLPs, annual review reports, Communication Profiles etc.).

17.4. Admin areas such as Assistant Heads', Pre-school, Acorn, and Head's offices & PIT & filing room cupboards will be locked overnight.

17.5. Surplus printouts of personal details/info to be shredded (cross-cut).

17.6. Digital data stored locally (i.e. on the server and Synology NAS backup drives) is password-protected. All data backed up to LGfL's cloud-based service Gridstore is encrypted before backup. Copies are kept for 60 days.

17.7. Memory sticks or portable storage devices will not be used to hold personal information unless they are password-protected and fully encrypted.

17.8. All electronic devices are password-protected to protect the information on the device in case of theft.

17.9. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

17.10. Staff and governors will not use their personal laptops, computers, tablets or mobile phones for school purposes, unless via protected remote access to the server, or password-protected LGFL email service, with additional password protection on the device.

17.11. All necessary members of staff are provided with their own secure login and password, and a forced password change occurs at the beginning of the academic year. Minimum password complexity is enforced i.e. 12 or more characters in length & include a mix of upper & lower case letters and numbers. All necessary members of staff are provided with their own laptop, which is set not to save data locally. Staff laptops to be brought in weekly to install Windows updates & update antivirus software.

17.12. Password protected screensaver on desktops & personal laptops is set to come on after 5mins (not class laptops, which are always supervised, when they are on)

17.13. Computers are set to automatically shut down overnight, thus activating the encryption on appropriate machines.

17.14. Emails should not generally contain personal/confidential info/data - this includes first name together with surname/DoB/photo. Children should be referred to by initials in the Subject of the email; first names can be used in the body of the email. Where information needs to be shared, it will be saved to a shared area of the server. If documents with sensitive/personal information need to be shared outside of school to LA etc., secure email, e.g. USO-FX2 or encrypted storage devices must be used. However, parents/carers can give permission for non-sensitive data about their children to be shared with them via email. Part 2 Governors' minutes should be password-protected.

17.15. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

17.16. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

17.17. Hard copies of personal data (e.g. annual review papers, copies of addresses, name with surname and/or date of birth) should not be taken offsite by school-based staff unless authorised by the headteacher. Sensitive or personal data must not be stored on home PCs and must not be accessible to other members of the household.

17.18. Laptops and any school papers, even those that do not contain personal data should be stored out of sight, in transit, i.e. in car boot and should never be left in a car overnight. If staff need to leave data in a car, for a short period, they should do a dynamic risk assessment, and take precautions to reduce the risk of theft

17.19. Pre-school teams, Acorn teachers & admin staff who have authorisation, and who need to work with hard copies offsite, should minimise the use of personal data, e.g. storing data digitally, using initials or first names, and personal data being added later to documents digitally or on school site. When storing school papers, they must use the most secure area of the home, and personal data should be out of sight, ideally locked away in filing cabinet drawer/room/safe. Staff who regularly keep hard copies of personal data at home must store this in a locked filing cabinet. The person taking the information from the school premises accepts full responsibility for the security of the data.

17.20. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

17.21. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

17.22. The physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

17.23. **Oakleigh & EYC** takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

17.24. The DPO is responsible for continuity and recovery measures are in place to ensure the security of protected data. Regular backups will be made and kept along with essential paper documents, so school could carry on in case of crisis, e.g. fire/flood

18. Sharing information

18.1. Care should be taken when sharing personal information internally - only share information that needs to be shared to that person. No casual sharing of information about a child or their family.

18.2. Information should only be shared with other professionals or external agencies, whose identity has been checked and who have a valid professional reason to have this information or immediate family members of the child concerned.

18.3. Information must be shared securely, according to the terms of this policy

18.4. **Oakleigh** will not publish any personal information, including photos, on its website without the permission of the affected individual.

19. Photography

19.1. The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

19.2. If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

19.3. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

20. Data retention

20.1. Data will not be kept for longer than is necessary.

20.2. Unrequired data will be deleted as soon as practicable.

20.3. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

20.4. Paper documents will be shredded or pulped. Electronic data stored on hard drives installed in obsolete machines will be securely wiped/sanitised or destroyed by a certified waste management company. Re-usable USB flash drives will be securely wiped before re-using and unwanted drives destroyed, once the data should no longer be retained.

21. DBS data

21.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

21.2. Data provided by the DBS will never be duplicated.

21.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

22. Policy review

22.1. This policy is reviewed every **two years**.

The next scheduled review date for this policy is **May 2020**.

Reviewed by Richard O'Connell June 2018