Oakfield Junior School

Data Protection Policy

Policy Number	OJS1015
Version Number	3.1
Policy Owner	Data Protection Officer
Governing Body or Working Group Approval	FGB
Adopted	Summer 2019
Review Date	Summer 2020

Contents

1. Aims

The school is required as part of its overall information governance structure to ensure that appropriate controls are implemented and maintained in relation to the collection, use and retention of personal information pertaining to its pupils, parents, schools workforce and contractors; and that these are in accordance with the requirements of the current data protection law as enacted. (The Data Protection Act 2018 and the Applied GDPR)

This document provides a framework for School workforce to meet legal and corporate requirements in relation to information requests that fall within the scope of the legislation.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

It must be noted that compliance is a legal requirement and that individuals can face prosecution for breaches of its Principles.

2. Legislation and guidance

This policy meets the requirements of the current data protection law as enacted (The Data Protection Act 2018 and the Applied General Data Protection Regulations (GDPR)). It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username

	It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who

	processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Gillian Ward and is contactable via the school office alternatively contact: Karen Tranter Admin and HR manager

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's *Information and Records Management Society's toolkit for schools* .

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned

- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should be submitted in writing, either by letter, email or fax to the Data Protection Officer. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or voluminous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to our site manager.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

All schools add and adapt to reflect your school's uses of photographs and videos for communication, marketing and promotional materials:

Uses may include:

- Within school on display boards, notice boards and in school brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified Data Protection Officer, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office

- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our policy on acceptable use)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection forms part of our continuing professional development and regular training (annually at first and then every two years) members of staff on data protection law, this policy, any related policies and any other data protection matters will take place or where changes to legislation, guidance or the school's processes make it necessary.

The school will also maintain a record of attendance at training events linked to Data Protection.

The school will regularly (annually at first and then every two years) conduct reviews and audits to test our privacy measures and make sure we are compliant.

18. Monitoring arrangements
The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually at first and then **every 2 years** and shared with the full governing board.

19. Links with other policies
This Data Protection Policy is linked to our:

- Freedom of information publication scheme
- Acceptable use of ICT Policy
- Child protection and Safeguarding Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the school's computer system. The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

Other types of breach could include:

- *Details of pupil premium interventions for named children being published on the school website*
- *Non-anonymised pupil exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*

DATA PROTECTION ACT 2018 – SUBJECT ACCESS REQUEST

Dear Mr _____

Thank you for your request which we received on_____. Your request falls under the Data Protection Act 2018 as your request is for personal information concerning your child.

We do take the handling of personal data seriously and we ask you to please provide two proofs of ID such as a copy of your passport/birth certificate and a copy of proof address such as a utility bill. This is to ensure that we are sending personal data to the right individual.

In order for us to process your request efficiently, it would be most helpful if you can specify the date range that you require information for and any particular information that you require. As you can understand there is a large amount of information held and we wish to ensure that you are supplied with the relevant information.

On receipt of the above ID we will process your request within the one month statutory reply period.

Yours Sincerely,

Dear

RE: YOUR REQUEST UNDER THE DATA PROTECTION ACT 2018

Thank you for your subject access request dated XXXX. Subject access requests are for personal data about the requester that is focused on the requester. It is for data/information and not the documents in which the data/information is found.

You have been quite specific in your request, which was for the following information held by the school:

STATE REQUEST

We searched our relevant systems to locate data within the scope of your request. The data retrieved was reviewed by the Senior Management to ensure it was your personal data.

- I confirm that we are processing the personal data specified in your request.

I enclose with this letter a copy of the document/s specified in your request.

We have redacted any reference to third parties where applicable and where we owe a duty of confidentiality.

I hope that the information attached satisfies your request.

If you are unhappy with the contents of the information provided, its accuracy or retention, or with the handling of your request, then you should raise this by writing to the Chair of Governors.

If, following this, you are not satisfied by the School's response to your complaint, you have the right to apply to the Information Commissioner for a decision. The Information Commissioner will normally expect you to have exhausted our complaints procedure. The Information Commissioner can be contacted at the Cheshire address below.

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

We supply this information based on your original request. Please do not hesitate to contact me at the above address, should you have any queries regarding the information enclosed.

Yours sincerely,

Headteacher

Information you hold										
What is the data?		**Why is it processed?**	**Whose is it?**		**When is it processed?**					**Where is it processed?**
Type	**Source**	**Lawful basis**	**Who**	**Reason for processing**	**Obtained/ updated**	**Disclosed to**	**Why is it disclosed**	**Retention period**	**How is retention period determined?**	**Paper/electronic/ data system etc**
Eg Special Educational	Parents, staff, external	Necessary for compliance with legal obligation	pupils	Legal obligation, provision of appropriate support	Admission to school and updated throughout year	Parents, staff, external agencies	Ensure support and provision is mapped and made known to relevant people	Until pupil leaves	No longer required	Paper in locked cupboard in SENCO office. Electronic on school network for SLT access.

Child's name: ……..

Child's Class: ……..

Photographic Images of Children – Consent form

To comply with the Data Protection bill 2018, we need your permission to photograph or make any recording of your child.

The table below shows the different ways your child's image/name may be used. Please tick to confirm your consent or otherwise for each medium, sign

What	Where	Yes	No
Your child's image and name	In school *e.g. display boards*		
Your child's name or image *Unidentifiable by full name and photograph combined unless agreed in advance with an adult with parental responsibility*	School publications *e.g. newsletter, DVD*		
Your child's name or image *Unidentifiable by full name unless agreed in advance with an adult with parental responsibility*	School online publications *e.g. website, app*		
Your child's image *Without name*	School social media *e.g. Facebook*		
Your child being photographed or filmed *News media may publish pictures along with the child's full name, but the school will seek an undertaking that a child's name will not be used if their image is put on the newspaper's own website.*	External press/media *e.g. newspapers, television images*		

and date the form and return it to your school office as soon as possible.

Declaration: I have read and understood the consent asked of me above. My decision on whether to give consent will remain valid throughout my child's time in their current key stage, unless I notify the school of the contrary in writing. I promise

that if I, or members of my family, take photographs or video recordings at a school event, these will be kept for family use only and will not be uploaded to social media .

Parent Name: _____

Parent _____

Date: _____

Appendix 2: Oakfield Junior School Job Description: Data Protection Officer

Responsible to: Governing Body and Headteacher

Purpose of the Job: To ensure the school complies with its legal obligations under the Data Protection Act 2018 and the Applied GDPR by developing, implementing and managing appropriate data protection practices within the school and providing specialist advice to others.

Key duties and responsibilities:

1. To provide specialist advice, guidance and training to SMT, governors and employees regarding their legal obligations under the Data Protection Act 2018 and the Applied GDPR and promote good practice in data protection management

2. Develop, implement and enforce suitable and relevant Data Protection policies and practices and ensure these are reviewed on an annual basis

3. To monitor compliance with the Data Protection Act 2018 and the Applied GDPR and other data protection provisions, undertaking internal audits and managing data protection risks reporting to SLT and Governors as appropriate

4. To coordinate internal data collection, processing and retention activities in accordance with the Data Protection Act 2018 and Applied GDPR provisions, maintaining comprehensive records of all data processing activities

5. Process, co-ordinate and respond to all requests for information in accordance with the Data Protection Act 2018 and the Applied GDPR or FOI provisions keeping a log of requests received

6. To be the first point of contact for supervisory authorities, external agencies and for individuals whose data is processed

7. To provide advice or undertake data protection impact assessments as required

8. To ensure any data breaches are investigated and remedial actions taken, reporting breaches to the ICO in accordance with legal requirements

9. To ensure all school documents / policies are compliant with Data Protection Act 2018 and the Applied GDPR provisions and contain appropriate privacy notices where required

10. To ensure records management and paper / electronic record keeping practices are compliant with GDPR requirements and review / revise as appropriate

11. To keep appraised of any changes to data protection / management requirements and ensure school practices are reviewed accordingly

12. To seek guidance from appropriate specialist agencies as required and to identify / coordinate the provision of specialist training on specific aspects of data protection / management as appropriate

Appendix 2: Data Protection Officer's Termly Report to FGB

Oakfield Junior School

GDPR Report to Governors

Autumn/Spring/Summer Term 20XX

Data Protection Officer: XXX

School GDPR Leads: Admin - XXX
Curriculum - XXX

Areas of strength within the school:

- XXX

Priorities for improvement:

- XXX

Spring Term Update:

- XXX
- XXX

Completed by: …… Date: …….