OWSLEBURY PRIMARY SCHOOL
POLICY DOCUMENT

NO. E150 – GDPR POLICY

Review History

March 2020	New Policy	March 2021
Autumn 2021	Review	Autumn 2022
Autumn 2022	Review	Autumn 2023
Spring 2024	Review	Spring 2025
Spring 2025	Review	Spring 2026

General Data Protection Regulation Policy

Our aims are to:

To ensure that all personal data collected about colleagues, pupils, parents, governors, visitors and other individuals is, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

Data Protection Act 2018 (DPA 2018)

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

Contents.

Appendices:

1. Legislation and guidance

This policy meets the requirements of the:

1. UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
2. Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

2. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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 • Criminal Records
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 organization that determines the purposes and the means of processing of personal data.
Data processor	A person, third party contractor, 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.

3. 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 (Registration reference: Z5178467) and will renew this registration annually or as otherwise legally required.

4. Roles and responsibilities

This policy applies to **all staff** employed at Owslebury Primary School, volunteers and external organisations or individuals working on our behalf. Colleagues who do not comply with this policy (with attention to Appendix One: Data Protection Responsibilities – For All Staff) may face disciplinary action, in accordance with the school (Model) Code of Conduct Policy.

4.1 Governing body

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection and with demonstrating their commitment to these obligations. All Governors communication is completed via Governor Hub, no emails are used.

4.2 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. Jo Saxby (01962 777452) is the appointed DPO at Owslebury Primary School.

They will provide a report of their activities directly to Governors Resources Committee and, where relevant, report to the Full Governing Body for 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 Roles and Responsibilities can be found at Appendix Two.

4.3 Headteacher.

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

4.4 All staff.

All colleagues working at Owslebury Primary School and volunteers, have a personal responsibility to keep person identifiable information and sensitive school information secure and confidential always:

Key Staff Data protection responsibilities are outlined at Appendix One.

5. Data protection principles

The UK & EU 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 and 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.

6. Collecting personal data

6.1 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**. A checklist for seeking consent to process personal data, can be found at Appendix Three.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020Data Protection Act 2018 (DPA 2018)

6.2 Online Services.

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).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

6.3 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 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 Local Authority School Records Retention Schedule Retention Policy.

7. 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. An example of our Third-Party Data Agreement can be found at Appendix Four
    - 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 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.

8. Subject access requests and other rights of individuals

8.1 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

It will be easier to recognise and respond to requests if they are in a consistent format, therefore Subject Access Requests must be submitted in writing, and using the template at Appendix Five: Subject Access Request form will greatly assist this process. This can then be emailed or faxed to the DPO, or alternatively it can be handed into the main office. Forms should include:

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

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

8.2 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.

8.3 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 numerous. 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 considers 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.

8.4 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 6), 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 based on 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.

9. 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.

10. 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.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

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

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 Policy for more information on our use of photographs and videos.

Our consent form for taking and using photos/ videos – can be found at Appendix Six.

11. 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:

- A suitably qualified DPO, has been appointed, who will have the necessary resources to fulfil their duties and maintain their 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 Data Privacy Impact Assessments (DPIA) where the school's processing of personal data presents an elevated risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process). Our Privacy impact assessment template can be found at Appendix Seven
- Integrating data protection into internal documents including this policy, any related policies. Our Privacy notices, which will be displayed on the school website can also be found at:
    - Appendix Eight: Owslebury Primary School Privacy Notice (Parents and Pupils)
    - Appendix Nine: Owslebury Primary School Privacy Notice (Workforce)
- 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

12. 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
- Staff are to ensure confidential information is shredded when no longer needed. Shredding bags must also be secured.
- Care must be taken to ensure pupil information is not accidently displayed on screens
- 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/ devices 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 online safety policy/ICT policy)
- 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 7)

13. 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.

14. 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 Personal Data Breach Procedure set out in Appendix Ten.

When appropriate, we will report the data breach to the ICO within 72 hours, using the template found at Appendix Eleven. 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

15. Training

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

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

16. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice.

17. Links with other policies

This data protection policy is linked to:

- Safeguarding policies
- HCC Retention Schedule
- School (Model) Code of Conduct Policy
- Online safety policy/ICT policy

Appendix One: Data Protection Responsibilities – For All Staff

All colleagues working at Owslebury Primary School, Wraparound provision (after school clubs) and volunteers have a personal responsibility to keep person identifiable/ sensitive information secure and confidential always:

Key responsibilities:

- Under UK & EU GDPR colleagues should be doing everything to prevent a breach of personal data
- Ensuring the security of personal data access from own devices:
    - Such as laptops or phones, to prevent the data from being lost, stolen or accidentally leaked.
    - Colleagues are not to share any devices that store personal data among family and friends.
    - Make sure antivirus software is installed on personal laptops and computers. Keep it up to date and ensure it makes regular scans.
- Keep the device password-protected:
    - All devices should be locked using a strong password or a PIN, to prevent others from accessing data through them
    - Strong passwords are at least 7 characters, with a combination of upper and lower-case letters, numbers and special keyboard characters (e.g. an asterisk or currency symbols)
    - If a wrong password or PIN is entered too many times, access to the device should be locked, or data stored in it should be automatically deleted
- Staff, pupils and contractors are not permitted to introduce or use any removable media, such as memory stick or hard drives, unless it is an **encrypted** device, with considerable care taken for its security
- Teaching colleagues must take care to ensure that pupils information is not accidently displayed on screens in classrooms, eg tutor registration
- Do not open any hyperlinks in emails or any attachments to emails, unless the source is known, trusted and expected
- Careful consideration will still need to be given with regards to why, whose, what and where the email is being sent - particularly when this pertains to personal information
- Locking computers. Accounts must be locked when moving away from a logged in terminal when left unattended, even for short periods of time - to prevent unauthorized access
- Collecting, storing and processing any personal data on school IT systems in accordance with this policy; colleagues must only process personal data, including photos, where it is necessary to do their jobs
- When staff no longer needs the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Local Authority School Records Retention Schedule Retention Policy.
- Staff must Inform the school of any changes to their personal data, such as a change of address, as soon as possible

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data must be kept secure when not in use. Staff must ensure that confidential info is shredded when no longer needed. Shredding bags must also be secured.
- 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 either the school office or medical room (eg medical care plans)
- Contact 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 there are any concerns that this policy is not being followed
    - If colleagues are unsure whether they have a lawful basis to use personal data in a certain way
    - If colleagues 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 or, potential breach
    - Whenever they are engaging in a recent activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties
    - Application of standalone learning application requiring a third-party Data processor
    - On receipt of any Subject Access Requests – an example of which is a pupil's behaviour record – these must be handled through the HT and DPO
    - All members of staff must also be aware of potential data breaches occurring using social media and must refer to the schools 'safer use of IT policy' in conjunction with this policy

Appendix Two: DPO's Roles and Responsibilities

Purpose.

The DPO is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee the school's data protection processes and advise the school on best practice.

Key responsibilities:

- Advise the school and its employees about their obligations under current data protection law, including the General Data Protection Regulation (UK & EU GDPR)
- Develop an in-depth understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures
- Monitor the school's compliance with data protection law, by:
    - Collecting information to identify data processing activities
    - Analysing and checking the compliance of data processing activities
    - Informing, advising and issuing recommendations to the school
    - Ensuring they remain an expert in data protection issues and changes to the law, attending relevant training as appropriate
- Ensure the school's policies are followed, through:
    - Assigning responsibilities to individuals
    - Awareness-raising activities
    - Co-ordinating staff training
    - Conducting internal data protection audits
- Advise on and assist the school with carrying out data protection impact assessments, if necessary
- Act as a contact point for the Information Commissioner's Office (ICO), assisting and consulting it where necessary, including:
    - Helping the ICO to access documents and information
    - Seeking advice on data protection issues
- Act as a contact point for individuals whose data is processed (for example, staff, pupils and parents), including:
    - Responding to subject access requests
    - Responding to other requests regarding individuals' rights over their data and how it is used
- Take a risk-based approach to data protection, including:
    - Prioritising the higher-risk areas of data protection and focusing mostly on these
    - Advising the school if/when it should conduct an audit, which areas staff need training in, and what the DPO role should involve
- Report to the governing body on the school's data protection compliance and associated risks
- Respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role

- Undertake any additional tasks necessary to keep the school compliant with data protection law and be successful in the role
- Maintain a record of the school's data processing activities
- Work with external stakeholders, such as suppliers or members of the community, on data protection issues

- Take responsibility for fostering a data protection culture throughout the school. Work closely with other departments and services to ensure GDPR compliance, such as HR, legal, IT and security

Appendix Three: A checklist for seeking consent to process personal data

Action	
Deciding whether you need to seek consent	
We have checked that consent is the most appropriate lawful basis for processing. The School only needs to seek consent where none of the other lawful bases apply. For example, ask for consent to: • Using photographs or videos of pupils on your school's website or other promotional material • Sending marketing material to prospective parents • Sending fundraising requests to alumni Examples where consent is not required as it is covered by our other 'lawful bases' (legal reasons) to do so under data protection law, are: • Sharing child protection concerns and records with the appropriate people or agencies (a specific document is used for police requests) • Submitting census data to the Department for Education	
Asking for consent (refer to these actions when writing a consent form)	
We have made the request for consent clear and separate from other terms and conditions	
We ask people to positively opt in	
We don't use pre-ticked boxes, or any other type of consent by default	
We use clear, plain language that is easy to understand	
We specify why we want the data and what we're going to do with it	
We give separate options to consent to the different things we will do with the data For example, if you're asking for consent to take photographs of children, ask parents to agree to each thing the photograph will be used for: "I am happy for the school to take photographs of my child. I am happy for photos of my child to be used on the school website. I am happy for photos of my child to be used in the school prospectus"	

We have named our organisation and any third parties that process the data	
We tell individuals they can withdraw their consent	
We ensure that the individual can refuse to consent without detriment	
We don’t make consent a precondition of a service	
Recording consent	
We keep a record of when and how we got consent from the individual	
We keep a record of exactly what they were told at the time	
Managing consent on an ongoing basis	
We regularly review consents to check that the relationship, the processing and the purposes have not changed	
We have processes in place to refresh consent at appropriate intervals, including any parental consents	
We make it easy for individuals to withdraw their consent at any time, and publicise how to do so	
We act on withdrawals of consent as soon as we can	
We don’t penalise individuals who wish to withdraw consent	

Appendix Four: Third-Party Data Agreement

Data Protection Contract Clauses for Owslebury Primary School – Third Party agreement.

1. The Supplier shall ensure that its staff, representatives and agents comply with the requirements of the Data Protection Act 1998 and the General Data Protection Regulation and any successor legislation (the Data Protection Legislation) when collecting or using the personal or special category data for the provision of the Services and shall not knowingly or negligently place the School in breach, or potential breach, of the Data Protection Legislation.

2. The Supplier is permitted to collect and use the following data but only to the extent necessary for the provision of the Services and only in accordance with documented instructions from the School and for no other purpose whatsoever except as required by law to act without such instructions ***(see Note 1 below)***:-

Personal Data	Special Category Data
Names	*Racial / ethnic origin*
Addresses	*Political opinions*
Email addresses	*Religious or philosophical beliefs*
Telephone number	*Trade union membership*
	Genetic data
	Biometric data
	Health data
	Data concerning sex life or sexual orientation

3. The Supplier is only permitted to collect and use the information described in clause 2 in respect of the following data subjects ***(see Note 2 below)***:-

- Pupils
- Parents
- School Staff
- Visitors
- Professional advisers

4. The Supplier shall obtain specific prior written authorisation from the School before engaging a subcontractor to provide any of the Services and shall oblige that subcontractor to fully comply with the requirements of the Data Protection Legislation by imposing the same data protection obligations within the subcontract as are contained in this Contract.

5. No personal information shall be disclosed to any other third party without first consulting the School regarding the legality and mechanism of the disclosure and obtaining the School's written authorisation confirming it is satisfied that there is a legal basis permitting the disclosure of the data, and that the disclosure mechanism is appropriate.

6. On termination of this Contract the Supplier shall return all personal data to the School or destroy or dispose of it in a secure manner and in accordance with any specific instructions issued by the School and shall confirm to the School that it has done so.

7. The Supplier shall give all reasonable assistance to the School necessary to enable the School to comply with its obligations under the Data Protection Legislation.

8. The Supplier shall comply with the School's security requirements and instructions, and shall have appropriate technical and organisation safeguards in place to protect the data and to meet the obligations imposed on it and the School by the Data Protection Legislation.

9. The Supplier shall, upon reasonable notice, allow officers of the School or an auditor appointed by the School, to have reasonable rights of access to the Supplier's premises, staff and records for the purposes of monitoring the Supplier's compliance with its security requirements and with the Data Protection Legislation.

10. The Supplier shall take reasonable steps to ensure the reliability of its staff accessing the School's data and shall ensure that they receive appropriate training in data protection to understand the confidential nature of the data and the need to comply with Data Protection Legislation. The Supplier shall ensure that it, its staff, representatives, agents and visitors will not access, read, listen to or in any way use School data unless it is necessary to do so for the provision of the Services and they have committed themselves to confidentiality.

11. The Supplier shall ensure that no personal data is transferred to a country or territory outside the European Economic Area and that no other data is transferred to a country or territory outside the European Economic Area without the prior written authorisation of the School.

12. The Supplier agrees to indemnify the School against all costs, claims and liabilities incurred by the School as a result of the Supplier's and / or the Supplier's Subcontractor's failure to comply with Data Protection Legislation as required by this Contract.

13. The Supplier shall notify the School within 24 hours if it becomes aware of a breach or potential breach of Data Protection Legislation.

14. In the event that the Supplier fails to comply with these terms, the School reserves the right to terminate this Contract, in whole or in part, in writing with immediate effect.

Note 1 *– The GDPR requires that types of personal data to be processed must be set out in contracts between data controllers and data processors (in most cases a school will be a data controller and a supplier will be a data processor). Please list the type of personal data which will be accessed and used in any way by the Supplier under the contract. You will need to delete any that are not relevant from the examples provided. For special category data, we suggest you simply list the data processed by the Supplier by reference to the categories only (as shown in the examples) and delete any that are not applicable.*

Note 2 *– The GDPR requires that categories of data subjects whose personal data is to be accessed and used by the supplier are listed in the contract. Please add to or delete the categories of data subjects as applicable.*

School:	***Third Party***
Jo Saxby	*Name:*
Data Protection Officer, on behalf of HT	*Appointment:*
Owslebury Primary School, Winchester	*Company/ Organisation:*
	Date: *Signature:*

Appendix Five: Subject Access Request Form

Dear Data Protection Officer,

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me and verify the lawfulness of the processing.

Under the GDPR, this information will be provided free of charge, and in most cases, must be provided within 1 month, unless the request is complex and numerous – notification will be given on this eventuality.

Here is the necessary information (To be completed/ supplied by person making request):

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:*

All Subject Access Requests require Head Teacher sign-off.

Name: *Signature:* *Date:*

Appendix Six

Using images of children

Multimedia consent form for use by

Hampshire County Council schools

To Name of the child's parent or guardian: _____

Name of child/ren _____

School Owslebury Primary School

Occasionally, we may take photographs of the children at our school. We may use these images in our school's prospectus or in other printed publications that we produce, as well as on our website or on project display boards at our school. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use.

From time to time, our school may be visited by the media who will take photographs or film footage of a visiting dignitary or other high profile event. Pupils will often appear in these images, which may appear in local or national newspapers, or on televised news programmes.

To comply with data protection legislation, we need your permission before we can photograph or make any recordings of your child for promotional purposes. Please answer questions 1 to 6, then sign and date the form where shown.

The information you provide (address, contact numbers) will be securely stored and processed within the EEA and not be used for any other purpose than confirming your permission to use the material.

Please return the completed form to the office

Conditions of use

This form is valid for the period of time your child attends this school. The consent will automatically expire after this time unless you have agreed for us to use photographs and images for a further 2 years after they have left our school. (2a / 3a)

We will not use the personal details or full names (which means first name and surname) of any child or adult in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications without good reason. For example, we may include the Christian name of a pupil in a newsletter to parents if the pupil has won an award.

If we name a pupil in the text, we will not use a photograph of that child to accompany the article without good reason.

We will not include personal e-mail or postal addresses, or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.

We may include pictures of pupils and teachers that have been drawn by the pupils.

We may use group or class photographs or footage with very general labels, such as 'a science lesson' or 'making Christmas decorations'.

We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

Your consent can be withdrawn at any time in writing.

Please note that the press has some exemptions from data protection legislation and may want to include the names and personal details of children and adults in the media.

I /we have read and understood the conditions of use and give my consent for my child's image/s to be used as described on the page overleaf.

I/we will not share images of children from Owslebury Primary School on social media sites without their parents' consent.

Your signature ……..…….. Date ……...

Please complete the form overleaf

	Please circle your answer
1. May we use your child's photograph on project display boards and in our Year book?	**Yes / No**
2.May we use your child's photograph in printed publications we produce for promotional purposes? eg. Prospectus, promotional 2a May we keep your child's photograph in printed publications after they have left our school for a period of 2 years?	**Yes / No** **Yes / No**
3.May we use your child's image on our website? 3a May we keep your child's image on our website after they have left our school for a period of 2 years?	**Yes / No** **Yes / No**
4. May we record your child's image on video or webcam for internal use? eg drama, PE lessons	**Yes / No**
5. Are you happy for your child to appear in the media? Please note this may link to the newspaper's online version.	**Yes / No**
6. Are you happy for your child to appear on Social Media sites used by the school e.g. Twitter, Facebook, YouTube - *Please note that once images are uploaded, they will be subject to the terms and conditions of the social media site. Neither you nor the school will have control over how those images are further used, amended or reproduced, either by the site or by the public. Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.*	**Yes / No**

Appendix Seven: Data Privacy Impact Assessments (DPIA) template

Checklist

Project name:

Brief description of project:

1. What is the project for? What does it seek to achieve?
2. Will the project collect information about individuals e.g. students, parents, staff? If no personal information is collected, a DPIA will not be required.
3. What type of information will it collect? Will it be special category data? e.g. information about an individual's physical or mental health, social care details, details of criminal offences or allegations, or collecting large quantities of personal information? Any of these will raise the level of risk.
4. How will the information be collected? On paper forms? Electronically? Who will have access to this information? How will it be stored and kept secure?
5. How will pupils/staff /parents be made aware of how their personal information is being used? Will a privacy notice be provided? At the end of a paper form? By

linking to the school website privacy notice? Does the privacy notice provide sufficient detail about the reasons for collecting the information and who it may be shared with?
6. Do you need consent from the individual to use the information? e.g. because special category data is being collected.
7. Does the project involve the use of new or different technology which could be privacy intrusive e.g. CCTV, monitoring of staff, biometrics, GPS tracking or cloud storage
8. What risks have been identified? What steps have been taken to eliminate or minimise them?
Signature Name (printed) Position Date

Appendix Eight.

Owslebury Primary School

Privacy Notice for Parents and Pupils

(How we use personal information)

1 The categories of personal information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Relevant medical information, Special Educational needs information and exclusions / behavioural information
- Assessment information

2 Why we collect and use this information

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services and how well our school is doing
- statistical forecasting and planning
- to comply with the law regarding data sharing

3 The lawful basis on which we use this information

The General Data Protection Regulation allows us to collect and use pupil information with consent of the data subject, where we are complying with a legal requirement, where processing is necessary to protect the vital interests of a data subject or another person and where processing is necessary for the performance of a task carries out in the public interest or in the exercise of official authority vested in the controller. When the personal information is Special Category Information we may rely on processing being in the substantial public interest in addition to consent of the data subject and the vital interests of the data subject or another.

Our requirement for this data and our legal basis for processing this data includes the Education Act 1996, 2002 and 2011, The childrens Act 1989 and 2004, Education and Skills Act 2008, Schools Standards and Framework Act 1998 and the Equalities Act 2010.

Owslebury Primary School collects and uses pupil information to comply with legal obligation and protection of vital interests.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this. Where we are using your personal information only on the basis of your permission, you may ask us to stop processing this information at any time.

4 Storing pupil data

We hold pupil data in accordance with out Records Retention schedule which can be found at: http://intranet.hants.gov.uk/school_records_retention_schedule.doc

5 Who we share pupil information with

- schools that the pupil's attend after leaving us
- our local authority
- Children's Services
- the Department for Education (DfE)
- Health professionals (school nurse, educational psychologist, speech and language, CAMHS, EMTAS)
- SEND professionals of educational settings

6 Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

7 Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools..

8 The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

9 Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact **The Data Protection Officer in the School Office.**

You also have the right, subject to some limitations to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress

- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

10 Contact

If you would like to discuss anything in this privacy notice, please contact:

- **The Data Protection Officer, Owslebury Primary School, Beech Grove, Owslebury, Hampshire, SO21 1LS**
- **adminoffice@owslebury.hants.sch.uk**

Appendix Nine.

Owslebury Primary School Privacy Notice

(How we use school workforce information)

1. The categories of personal information that we collect, hold and share include:

- personal information (such as name, address, email, telephone number, mobile telephone number, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- relevant medical information
- payroll information
- references

2. Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- to comply with the law regarding checks such as DBS checks and medical clearance
- comply with guidance such as 'Working Together' and Safeguarding obligations
- Performance management reviews
- CPD and staffing issues
- payroll and pension contributions

If we are required to comply with other legal obligations not listed above, we will share data only when it is lawful to do so.

3. The lawful basis on which we process this information

We process this information under **:**

- **Article 6 (1) (b)** processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract.
- **Article9 (2) (b)** processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- Further information regarding data collection can be found in the Education Act 1996

within guide documents on the following website: http://www.gov.uk/education/data-collection-and-censuses-for-schools

4. Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

5. Storing this information

We hold school workforce data for the length of time you work for the school plus seven years (in accordance with the HCC Records Retention Schedule) after this period the files are destroyed.

6. Who we share this information with

We routinely share this information with:

- our local authority
- the Department for Education (DfE)

7. Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority
We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)
We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

8. Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

- To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote

the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

9. Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the administrative officer.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact:

- **The Data Protection Officer, Owslebury Primary School, Beech Grove, Owslebury, Hampshire, SO21 1LS**
- **adminoffice@owslebury.hants.sch.uk**

Appendix Ten: 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 later by the ICO or an individual affected by the breach. Documented decisions are stored on the school's backed up Data storage network GDPR area. The nominated Governor Data Protection Link along with the Headteacher will be notified.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours, using the templated Data Breach Reporting Form found at Appendix Thirteen. 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, cause and effect
    - 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 backed up Data storage network GDPR area. 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.

The following are our relevant actions we will take for different types of risky or sensitive personal data processed by your school.

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 our onsite IT support to attempt 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
- Loss of individual Medical care plans
- Loss of Personal folder/ information.

Appendix Eleven: 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 DPO 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	