WOODHAM WALTER C OF E (VC) PRIMARY SCHOOL

Nurturing Lifelong Learners

Data Protection Policy

"To know, value and nurture God's world and one another"

Approved by Governors December 2022

To Be Reviewed: December 2026

4 yearly

Contents

Part 1 Introduction and Key Definitions

1.1 Introduction

Woodham Walter C of E V/C Primary School needs to gather and use certain information about individuals.

These individuals can include pupils, parents/carers, employees, suppliers, business contacts and other people the Woodham Walter C of E V/C Primary School has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Woodham Walter C of E V/C Primary School data protection standards — and to comply with the law.

This data protection policy ensures Woodham Walter C of E V/C Primary School

- complies with data protection law and follows good practice
- protects the rights of pupils, staff, parents/carers and other stakeholders
- is open about how it stores and processes individuals' data
- protects itself from the risks of a data breach

This Data Protection policy is based on the six principles of the Data Protection Act (DPA) that personal data shall be:

1. processed lawfully, fairly and in a transparent manner
2. collected for specified, explicit and legitimate purposes
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. accurate and kept up to date
5. kept in a form which permits identification of data subjects for no longer than is necessary
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss or damage

1.2 Key Definitions

Data

The DPA describes how organisations, including Woodham Walter C of E V/C Primary School must collect, handle and store personal information ('data').

Data is any information that the school collects and stores about individuals or organisations. Some data is more sensitive than others and particular care will be given to processing and managing this. Sensitive data includes:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;

- data concerning health or sex life and sexual orientation;
- genetic data; and
- biometric data.

Data can be stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Data Subject

A 'Data Subject' is someone whose details the school/academy keeps on file. The data subject has the following rights under data protection legislation:

- to be informed
- to have access to data stored about them (or their children)
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for the school to keep their data
- to restrict processing (e.g. limit what their data is used for)
- to object to data being shared or collected

Although data protection legislation affords these rights to individuals, in some cases the obligations schools have to share data with the DfE etc override these rights (this is documented later in the policy under 'Privacy Notices').

Data Controller

The 'Data Controller' has overall responsibility for the personal data collected and processed and has a responsibility for ensuring compliance with the relevant legislation. They are able to delegate this to 'Data Processors' to act on their behalf.

The school governing body is the 'Data Controller'.

Data Processor

A 'Data Processor' uses, collects, accesses or amends the data that the controller is authorised to collect or has already collected. It can be a member of staff, third party company or another organisation such as the police or Local Authority (LA).

Part 2 Organisational Arrangements

2.1 Overall Responsibility

Woodham Walter C of E V/C Primary School will meet its obligations under the DPA by putting in place clear policies that focus on the key risks and in checking that control measures have been implemented and remain appropriate and effective.

2.2 Roles & Responsibilities

The Governing Body will:

- Establish and maintain a positive data protection culture.
- Ensure the Executive Headteacher prepares a Data Protection policy for approval and adoption by the governing body and to review and monitor the effectiveness of the policy.
- Appoint a Data Protection Officer and provide adequate resources and support for them to fulfil their statutory duties.
- Allocate sufficient resources for data protection, e.g. in respect of training for staff, encryption technology for devices.
- Monitor and review data protection issues.
- Ensure that the Woodham Walter C of E V/C Primary School provides adequate training, information, instruction, induction and supervision to enable everyone to comply with their data protection responsibilities.
- Review and act upon data protection compliance reports from the Data Protection Officer.

The Executive Headteacher will:

- Promote a positive data protection culture.
- Prepare a Data Protection policy for approval by the Governing Body revise as necessary and review on a regular basis, at least every two years.
- Ensure that all staff co-operate with the policy.
- Ensure that staff are competent to undertake the tasks required of them and have been provided with appropriate training.
- Provide staff with equipment and resources to enable them to protect the data that they are processing.
- Ensure that those who have delegated responsibilities are competent, their responsibilities are clearly defined, and they have received appropriate training.
- Monitor the work of the Data Protection Officer to ensure they are fulfilling their responsibilities.

The Data Protection Officer will:

- Inform and advise the Woodham Walter C of E V/C Primary School of their obligations under data protection legislation.
- Monitor compliance with the legislation and report to the Executive Headteacher and governing body on a termly basis.
- Cooperate with the supervisory authority (e.g. Information Commissioners Office) and act as the main contact point for any issues.
- Seek advice from other organisations or professionals, such as the Information Commissioners Office as and when necessary.
- Keep up to date with new developments in data protection issues for schools.
- Act upon information and advice on data protection and circulate to staff and governors.
- Carry out a data protection induction for all staff and keep records of that induction.
- Coordinate the school response to a Subject Access Request.
- Coordinate the school response to a data breach

Staff at the school will:

- Familiarise themselves and comply with the Data Protection Policy.
- Comply with the Woodham Walter C of E V/C Primary School data protection arrangements.
- Follow the data breach reporting process.
- Attend data protection training as organised by the school.

Part 3 Detailed Arrangements & Procedures

3.1 Data Management

Data Registration

As Data Controller, the school must register as a Data Controller on the Data Protection Register held by the Information Commissioner. The school renewed with the Data Controller on 09/06/2019.

Data Protection Officer

As a public body, Woodham Walter C of E V/C Primary School is required to appoint a Data Protection Officer (DPO).

At Woodham Walter C of E V/C Primary School the DPO role is fulfilled by:

- SBM services 01206 671103

The role of the DPO is to:

- Inform and advise the school/academy and the employees about obligations to comply with all relevant data protection laws.
- Monitor compliance with the relevant data protection laws.
- Be the first point of contact for supervisory authorities.
- Coordinate training on data protection for all key stakeholders in the Woodham Walter C of E V/C Primary School

Data Protection Awareness

In order to ensure organisational compliance, all staff and other key stakeholders (e.g. governors, volunteers) will be made aware of their responsibilities under the data protection legislation as part of their induction programme, (both as a new employee/governor to the organisation or if an individual changes role within the school/academy).

Annual data protection refresher training will take place to reinforce the importance of staff adhering to the legislation.

A record of the professional development undertaken by the individual will be retained on their training record.

Data Mapping

Woodham Walter C of E V/C Primary School has documented all of the data that it collects within a 'Data Flow Map'. This data inventory records:

- the data held
- what the data is used for
- how it is collected
- how consent is obtained
- how the data is stored
- what the retention period is
- who can access the data
- who is accountable for the data
- how the data is shared
- how the data is destroyed

For each data type, the probability of a data breach occurring is assessed (very high, high, medium, low or very low) and actions to be taken to mitigate the risk are recorded.

It is the responsibility of the DPO to ensure the 'Data Flow Map' is kept up to date. The map should be a live document and updated regularly.

3.2 Third Party Suppliers Acting as Data Processors

As Data Controller, the Woodham Walter C of E V/C Primary School is responsible for ensuring that correct protocols and agreements are in place to ensure that personal data is processed by all sub-contractors and other third parties in line with the principles of the data protection legislation.

Individuals within school who have a responsibility for securing contracts and agreements with such third parties are responsible for ensuring that all external data processing is contracted out in line with the principles of the DPA. These types of agreements include: -

- IT contracts and processes.
- Physical data and hard copy documents.
- Data destruction and hardware renewal and recycling financial and personnel information.
- Pupil and staff records.

Only third party suppliers who can confirm they have appropriate technical, physical and organisational security to securely process data will be considered as suitable partners.

The procurement process will ensure that all contracts are suitable and reflect DPA requirements. Review of current and due consideration of future contracts will require this even if data processing is ancillary to the main purpose of the contract.

The external processor will confirm with the data controller that suitable security and operational measures are in place.

Any potential supplier or purchaser outside the EU will be obliged to confirm how they comply with the DPA and give contractual assurances.

The DPO may require a specific risk assessment to be undertaken if the data is sensitive, and if an increased risk is likely due to the nature, or proposed nature, of the processing.

A written agreement will be in place between the supplier and the school to confirm compliance with the DPA principles and obligations to assist the school in the event of data breach or subject access request, or enquiries from the ICO.

The school must have the right conduct audits or have information about audits that have taken place in respect of the relevant processes of the supplier's security arrangements whilst the contract is in place, or whilst the supplier continues to have personal data that relates to the contract on its systems.

Any subcontracting must only be done with the written consent of the school as data controller. This must be the case for any further subcontracting down the chain. All subcontractors must confirm agreement to be bound by DPA principles when handling the school's data, which shall also include co-operation and eventual secure destruction or return of data.

The school has a 'Third Party Request for Information' form – Appendix A - which must be used for third party suppliers acting as a Data Processor for the school.

3.3 Consent

As Woodham Walter C of E V/C Primary School we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required. However, in most cases, data will only be processed if explicit consent has been obtained.

Consent is defined by the DPA as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

Privacy Notices

In order to comply with the fair processing requirements of the DPA, the school will inform their staff and parents/carers of all pupils of the data they collect, process and hold on them, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom their data may be passed, through the use of 'Privacy Notices'.

Privacy notices are available to staff and parents through the following means:

- School website
- School newsletter
- Letter to parents
- Staff Handbook
- Staff Notice Boards

The Use of Pupil Images

Occasionally the Woodham Walter C of E V/C Primary School may take photographs of its pupils. These images could be used as part of internal displays, printed publications, the school website or our social media accounts.

Woodham Walter C of E V/C Primary School will seek consent from all parents on entry to the school, to allow the photography of pupils and the subsequent reproduction of these images.

Parents are given the opportunity to opt in. It is not permissible to assume parents are opting in.

Generic consent for all uses of images is not acceptable; parents must give consent to each medium.

Parents must be given the opportunity to withdraw their consent at any time. This should be given in writing to the school; however, a verbal withdrawal of consent is also valid and should be reported to the School Business Manager immediately.

Consent should be recorded on Sims.

If images of individual pupils are published, then the name of that child should not be used in the accompanying text or caption unless specific consent has been obtained from the parent prior to publication.

Accurate Data

The school will endeavour to ensure that the data it stores is accurate and up to date.

When a pupil or member of staff joins the Woodham Walter C of E V/C Primary School they will be asked to complete a form providing their personal contact information (e.g. name, address, phone number, NI number for staff), next of kin details, emergency contact and other essential information. At this point, the Woodham Walter C of E V/C Primary School will also seek consent to use the information provided for other internal purposes (such as promoting school events, photography).

Parents/carers and staff are requested to inform the Woodham Walter C of E V/C Primary School when their personal information changes.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent, the school will consider each situation on the merits and within the principles of the DPA, child welfare, protection and safeguarding principles.

Parents/carers and staff are requested to complete a Withdrawal of Consent form - Appendix B - and return this to the School Business Manager

3.4 Associated Data Protection Policies

- Complaints
- Data Breaches
- Data Records Management & Retention
- Subject Access Requests
- Third Party Requests for Information
- Use of Personal Devices

Complaints

Complaints will be dealt with in accordance with the Woodham Walter C of E V/C Primary School Complaints Policy and Procedures. In the event that the issue is unresolved it should be referred to the ICO (Information Commissioner's Office) Tel: 0303 123 1113

Data Breaches

Although the Woodham Walter C of E V/C Primary School takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone).

- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space).
- Unforeseen circumstances such as fire or flood.
- Hacking attack.
- 'Blagging' offences where information is obtained by deceiving the Woodham Walter C of E V/C Primary School

The school has a Data Breach policy – Appendix D - which sets out the process that should be followed in the event of a data breach occurring.

Privacy Impact Assessments

When considering the purchase of a new service or product that involves processing personal data, a Data Privacy Impact Assessment must be completed by the DPO. If risks are identified as part of the assessment, then appropriate steps to mitigate this risk must be implemented. If these risks are deemed to be 'high risk' then the DPO should consult with the ICO prior to implementation.

The 'Data Privacy Impact Assessment' form – Appendix E -must be used for each new service/product.

Records Management

The Woodham Walter C of E V/C Primary School recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations which will also contribute to the effective overall management of the school.

The Woodham Walter C of E V/C Primary School has a Record Management & Retention policy in place which sets out how it will:

- safely and securely store data (both digital and hard copy data)
- retain data
- dispose of data

Subject Access Requests

Any individual, person with parental responsibility or young person with sufficient capacity has the right to ask what data the school holds about them, and can make a Subject Access Request (SAR).

The school has a Subject Access Request policy,- Appendix F - which sets out the process that should be followed in the event of receiving a SAR.

Third Party Requests for Information

Occasionally the Woodham Walter C of E V/C Primary School may receive a request for information on a pupil or member of staff by a third party, such as the police or social services. This would be separate to statutory requests that come through from the DfE or LA, for example, which are covered within the privacy notices.

The Woodham Walter C of E V/C Primary School has a Third Party Request for Information policy – Appendix G - which sets out the process that should be followed in the event of receiving a third party request.

Use of Personal Devices

The Woodham Walter C of E V/C Primary School recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices. The Woodham Walter C of E V/C Primary School follows the 'Bring Your Own Device' policy which sets out how non-school owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members and visitors to the school. Appendix G.

Appendices

Appendix A – Third Party Request for Information form

Appendix B – Withdrawal of Consent Form

Appendix C – Data Breach Policy

Appendix D – Data Privacy Impact Assessments

Appendix E – Subject Access requests

Appendix F – Bring your own device policy

Appendix A - Third Party Request for Information Form

This form should be completed where a third party contacts the school requesting that information is shared with them about a member of staff or a student.

Remember, the police and other agencies have processes that they need to follow in order to legitimately gain information that is protected within the Data Protection regulations. However, child protection and safeguarding take priority and if information is requested on an emergency basis where there is immediate or significant risk, information can be disclosed.

This form should be completed on receipt of an information request, with authority sought from Data Protection Officer –SBM Services 01206 671103/Executive Headteacher.

A copy should be retained on the relevant staff or pupil file.

Date of Request:	
Time of Request:	
Person receiving request:	
Position:	

Details of Third Party

Name:	
Position:	
Agency:	
How has request been made?	Face to face ☐ Telephone ☐ Letter ☐ Email ☐ Other (please describe)

Details of Information Requested

Data that has been requested:	
Reason the data has been requested:	

Authorisation to Release Information

Name:	
Position:	
Date:	
Time:	
Authority to release requested information?	Yes / No
Summary of Information to be released:	

Confirmation of Information Released:

Date Information Released:	
Time Information Released:	
Method of Releasing Information:	Face to face ☐ Telephone ☐ Letter ☐ Email ☐ Other (please describe)

Person who released the information:	
Position:	
Summary of Information Released:	
Follow Up Action to be Taken:	

Appendix B
Consent Withdrawal Form – on behalf of Pupil

Please read the following notes carefully before completing the form.

Please note that as a school we may have contractual, statutory and/or regulatory reasons why we will still process and hold details of a pupil, parent, staff member, volunteer or other person.

Where two parents share parental responsibility, or where PR is shared and the pupil is capable of expressing a view and there is conflict between the individuals, the process of withdrawing consent will be subject to an evaluation and discussion to enable a decision to be reached that is considered to be in the pupil's best interests.

We may need to seek identification evidence and have sight of any Court Order or Parental Responsibility Agreement in some cases to action this request. If this is the case, a senior member of school staff will discuss this with you.

Please complete and deliver this form to the school office with your signature.

Student Images

Please tick the boxes below to indicate from which of the Student Image mediums you wish to **WITHDRAW** consent:

	CONSENT WITHDRAWN
I withdraw permission for my child's photo to be used within school for display purposes.	☐
I withdraw permission for my child's photo to be used in their annual school report	☐
I withdraw permission for my child's photo to be used on the school website.	☐
I withdraw permission for my child's photo to be used in other printed publications.	☐
I withdraw permission for my child's photo to be used on the school's social media sites eg twitter	☐
I withdraw permission for my child to appear in the media.	☐
I withdraw permission for my child to have a school photograph taken.	☐
I withdraw permission for all of the above	☐

Marketing & Fundraising

This section refers to notifications of activities concerning school-based events (such as open mornings, Parent Association fundraising events, class assemblies) either by phone, text, emails or letters.

Please use the boxes below to indicate from which of the communication methods you wish to WITHDRAW your consent so that the school does NOT contact you for these purposes:

Phone Call: ☐

Text Message: ☐

Email: ☐

Letter: ☐

All of the Above: ☐

Direct Marketing

This section refers to notifications of special offers or promotions by certain third parties (for example companies offering discounted rates to families during school holiday periods, information about local events) either by phone, text, emails or letters.

Please use the boxes below to indicate from which of the communication methods you wish to WITHDRAW your consent so that the school does NOT contact you for these purposes:

Phone Call: ☐

Text Message: ☐

Email: ☐

Letter: ☐

All of the Above: ☐

This form is valid for the whole time that your child remains a pupil at our school unless a further written consent or withdrawal of consent form is received.

I confirm that I have parental responsibility for the pupil.

Parent/Carer Signature: _____ **Date:** _____

Print Name: _____

Pupil Name: _____ **Relationship to child:** _____

For office use only

Received by school

Name of staff

member:

Dated:

Actions:

Appendix C - Data Breach Policy and Process

Although the Woodham Walter C of E V/C Primary School takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space)
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the <school/academy>

However, the breach has occurred, the following steps should be taken immediately:

1. **Internal Notification:** Individual who has identified the breach has occurred must notify the Woodham Walter C of E V/C Primary School DPO. A record of the breach should be created using the following templates:
    a. Data Breach Incident Form (Appendix 1)
    b. Data Breach Log (Appendix 2)
    c. Evidence Log (Appendix 3)

2. **Containment:** DPO to identify any steps that can be taken to contain the data breach (e.g. isolating or closing the compromised section of network, finding a lost piece of equipment, changing access codes) and liaise with the appropriate parties to action these.

3. **Recovery:** DPO to establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g. physical recovery of equipment, back up tapes to restore lost or damaged data)

4. **Assess the risks:** Before deciding on the next course of action, DPO to assess the risks associated with the data breach giving consideration to the following, which should be recorded in the Data Breach Notification form (Appendix 3):

    a. What type of data is involved
    b. How sensitive is it?
    c. If data has been lost/stolen, are there any protections in place such as encryption?
    d. What has happened to the data?
    e. What could the data tell a third party about the individual?
    f. How many individuals' data have been affected by the breach?

g. Whose data has been breached?
h. What harm can come to those individuals?
i. Are there wider consequences to consider such as reputational loss?

5. **Notification to the Information Commissioners Office (ICO):** Following the risk assessment in step 4, the DPO should notify the ICO within 72 hours of the identification of a data breach if it is deemed that the breach is likely to have a significant detrimental effect on individuals. This might include if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage.

   The DPO should contact ICO using their security breach helpline on 0303 123 1113, option 3 (open Monday to Friday 9am-5pm) or the ICO Data Breach Notification form can be completed and emailed to casework@ico.org.uk.

6. **Notification to the Individual:** The DPO must assess whether it is appropriate to notify the individual(s) whose data has been breached. If it is determined that the breach is likely to result in a high risk to the rights and freedoms of the individual(s) then they must be notified by the Woodham Walter C of E V/C Primary School

7. **Evaluation:** The DPO should assess whether any changes need to be made to the Woodham Walter C of E V/C Primary School processes and procedures to ensure that a similar breach does not occur.

Appendix C - Data Breach Incident Form

Part 1: Breach Information

When did the breach occur (or become known)?	
Which staff member was involved in the breach?	
Who was the breach reported to?	
Date of Report:	
Time of Report:	
Description of Breach:	
Initial Containment Activity:	

Part 2: Breach Risk Assessment

What type of data is involved:	Hard Copy: Yes / No Electronic Data: Yes / No
Is the data categorised as 'sensitive' within one of the following categories:	Racial or ethnic origin: Yes / No Political opinions: Yes / No Religious or philosophical beliefs: Yes / No Trade union membership: Yes / No Data concerning health or sex life and sexual orientation: Yes / No Genetic data: Yes / No Biometric data: Yes / No
Were any protective measures in place to secure the data (e.g. encryption):	Yes / No If yes, please outline:
What has happened to the data:	
What could the data tell a third party about the individual:	
Number of individuals affected by the breach:	

Whose data has been breached:	
What harm can come to those individuals:	
Are there wider consequences to consider e.g. reputational loss:	

Part 3: Breach Notification

Is the breach likely to result in a risk to people's rights and freedoms?	Yes / No If Yes, then the ICO should be notified within 72 hours.
Date ICO notified:	
Time ICO notified:	
Reported by:	
Method used to notify ICO:	
Notes:	
Is the breach likely to result in a high risk to people's rights and freedoms?	Yes / No If Yes, then the individual should be notified
Date individual notified:	
Notified by:	
Notes:	

Part D: Breach Action Plan

Action to be taken to recover the data:	
Relevant governors/trustees to be notified:	Names:
	Date Notified:
Notification to any other relevant external agencies:	External agencies:
	Date Notified:
Internal procedures (e.g. disciplinary investigation) to be completed:	
Steps needed to prevent reoccurrence of breach:	

Appendix 2 - Data Breach Log

Date Reported:	Notified By:	Reported To:	Description of Breach:	Notification to ICO:	Notification to Individual(s)	Further Actions to be taken:	Reviewed by:
				Yes/No	Yes/No		
				Yes/No	Yes/No		
				Yes/No	Yes/No		

Appendix 3 - Data Breach: Evidence Log

Date:	Description of Evidence:	Details of where evidence is stored/located:	Member of staff who collected data:

A**ppendix D – Privacy Impact Assessments**

Part 1: Privacy Impact Assessment (PIA) screening questions

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

Question	Yes / No?	Notes
Will the project involve the collection of new information about individuals?		
Will the project compel individuals to provide information about themselves?		
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.		
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?		
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.		
Will the project require you to contact individuals in ways that they may find intrusive?		

Part Two: Privacy Impact Assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process that is used in this code of practice. You can adapt the process and this template to produce something that allows your organisation to conduct effective PIAs integrated with your project management processes.

Step One: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the school, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Part three can be used to help you identify the GDPR related compliance risks.

- Privacy Issue
- Risk to Individuals
- Risk to Compliance
- Risk to School

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).

- Solution(s)
- Result: is the risk eliminated, reduced or accepted?
- Risk
- Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

- Risk
- Approved solution
- Approved By

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

- Action to be taken
- Date for completion of action
- Responsibility for action

Contact point for future privacy concerns:

SBM Services 01206 671103

Part three: Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Question	Yes / No?	Notes
Have you identified the purpose of the project?		
How will you tell individuals about the use of their personal data?		
Do you need to amend your privacy notices?		
Have you established which conditions for processing apply?		
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?		
If your organisation is subject to the Human Rights Act, you also need to consider:		
Will your actions interfere with the right to privacy under Article 8?		
Have you identified the social need and aims of the project?		
Are your actions a proportionate response to the social need?		

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Question	Yes / No?	Notes
Does your project plan cover all of the purposes for processing personal data?		
Have you identified potential new purposes as the scope of the project expands?		

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Question	Yes / No?	Notes
Is the quality of the information good enough for the purposes it is used?		
Which personal data could you not use, without compromising the needs of the project?		

Principle 4

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

Question	Yes / No?	Notes
If you are procuring new software does it allow you to amend data when necessary?		
How are you ensuring that personal data obtained from individuals or other organisations is accurate?		

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

Question	Yes / No?	Notes
What retention periods are suitable for the personal data you will be processing?		
Are you procuring software that will allow you to delete information in line with your retention periods?		

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Question	Yes / No?	Notes
Will the systems you are putting in place allow you to respond to subject access requests more easily?		
If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?		

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Question	Yes / No?	Notes
Do any new systems provide protection against the security risks you have identified?		
What training and instructions are necessary to ensure that staff know how to operate a new system securely?		

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Question	Yes / No?	Notes
Will the project require you to transfer data outside of the EEA?		
If you will be making transfers, how will you ensure that the data is adequately protected?		

Appendix E - Subject Access Requests

Any individual, person with parental responsibility or young person with sufficient capacity has the right to ask what data the school/academy holds about them, and can make a Subject Access Request (SAR).

A SAR can be made using the 'Subject Access Request' form (Appendix 1a).

The DPO has been designated as the person who will coordinate the response to a SAR.

The school is required to provide the individual with the data it holds on them within one calendar month. An extension of up to one calendar month can be granted if a school closure period is scheduled to occur during the initial one calendar month response time.

The response to the SAR will be provided in an electronic form.

It is permissible to ask the individual who has made the request to be more specific about the information that they require in order to ensure that the information they are provided with meets their requirements rather than providing lots of information that may not be relevant to their query.

Evidence of the identity of the person making the request and their relationship to the pupil must be gained prior to any disclosure of information. This should be recorded on the SAR Log (Appendix B).

Exemptions to a SAR include:

- Education, Health, Social Work records
- Examination marks and scripts
- Safeguarding records
- Special educational needs
- Parental records and reports
- Legal advice and proceedings
- Adoption and Court records and/or reports
- Regulatory activity and official requests e.g. DfE statistical information
- National security, Crime and taxation
- Journalism, literature and art
- Research history, and statistics
- Confidential references

Appendix 1a - Subject Access Request (SAR) Form

Part A: Data Subject's Details (person whose information you are requesting)

Title:	
Full Name:	
Date of Birth:	
Address:	
Year Group (if pupil at school)	

Part B: Requestor Details

Title:	
Full Name:	
Address:	
Phone Number:	
Email Address:	
Evidence of Identity (e.g. passport, driving license):	Evidence Provided? Yes / No Details:
Status of Requestor:	Data Subject: Yes / No Parent or person with parental responsibility: Yes / No Other: Yes / No If you have selected 'yes' for 'Other', please outline your role here:

Part C: Details of Subject Access Request

Details of Data Being Requested:	

Part D: Declaration

Option i

I , ……., hereby request that Woodham Walter C of E V/C Primary School provide the data requested about me.

Signed:_____

Date:_____

Option ii

I , ……., hereby request that Woodham Walter C of E V/C Primary School provide the data requested about ……. (insert child's name) on the basis of the authority that I have.

Signed:_____

Date:_____

Appendix B

Data Subject	Request	Date of SAR	Date DPO notified	ID confirmed	Response Deadline	Extension to Deadline?	Data held by school	Any additional info from requestor?	Any info to be withheld?	Who auth'd with-holding info?	Response checked and approved by DPO
E.g. John Smith	All data held about this staff member	01/02/18	01/02/18	Passport seen 02/02/18	01/03/18	08/03/18: 1 week due to Feb ½ term.	Personnel file – hard copy Email correspondence about individual	JS clarified the request links to a grievance they have with their line manager	Redacted email correspondence to remove reference to other employees	DPO 20/02/18	DPO 01/03/18

Subject Access Request (SAR) Log

Appendix F – Bring Your Own Device Policy

Part 1 Introduction

Woodham Walter C of E V/C Primary School recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices.

This policy describes how non-school owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members and visitors to the school. This practice is commonly known as 'bring your own device' or BYOD, and these devices are referred to as 'personal devices' in this policy. If you are unsure whether your device is covered by this policy, please check with the Data Protection Officer.

Part 2 Organisational Arrangements

Overall Responsibility

The governing body of the Woodham Walter C of E V/C Primary School is responsible for the approval of this policy and for reviewing its effectiveness.

Roles & Responsibilities

Staff members will:

- Familiarise themselves with their device and its security features so that they can ensure the safety of school information.
- Install relevant security features and maintain the device appropriately.
- Set up passwords, passcodes, passkeys or biometric equivalents on the device being used.
- Set up remote wipe facilities if available, and implement a remote wipe if they lose the device.
- Encrypt documents or devices as necessary.
- Report the loss of any device containing school information, or any security breach immediately to the Data Protection Officer.
- Ensure that no school information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of / sold / transferred to a third party.

Visitors will:

- Familiarise themselves with the use of personal devices at the school.
- Only use personal devices for agreed purposes at the school and with parental or the relevant permission.
- Not share information from personal devices via social media and will not keep school information indefinitely.

Part 3 Detailed Arrangements & Procedures

Use of personal devices at the school

Staff and visitors to the school may use their own devices in the following locations:

- In the classroom with the permission of the teacher.
- In the school environments e.g. libraries, sports pitches and outdoor spaces.

Personal devices must be switched off when in a prohibited area, and / or at a prohibited time, and must not be taken into controlled assessments and / or examinations unless special circumstances apply.

The school reserves the right to refuse staff and visitors permission to use their own device on school premises.

Use of cameras and audio recording equipment

Parents and carers may take photographs, videos or audio recordings of their children at school events for their own personal use.

Other visitors and staff may use their own personal devices to take photographs, video, or audio recordings in school provided they have checked that parental permission has been received by the School. This includes people who may be identifiable in the background.

Photographs, video or audio recordings made by staff on their own devices should be deleted as soon as reasonably possible after they have been used, e.g. uploaded for use on one of the school's social media sites. Photographs, video or audio recordings to be retained for further legitimate use, should be stored securely on the school network.

Photographs, video or audio recordings should not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them.

Devices must not be used to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video or audio recordings in school.

Access to the schools' internet connection

The school provides a wireless network that staff and visitors to the school may use to connect their personal devices to the internet. Access to the wireless network is at the discretion of the school, and the school may withdraw access for anyone it considers is using the network inappropriately.

The school cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's network. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's network.

Access to the school's systems

Staff are permitted to connect to or access the following school services from their device:

- The school email system.
- The school management information system.

Staff may use the systems to view school information via their personal devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their device. In some cases, it may be necessary for staff to download school information to their personal devices in order to view it (e.g. an email attachment). Staff shall delete this information from their device as soon as they have finished viewing it.

Staff must only use the IT systems and any information accessed through them for work purposes. School information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to, or distribution of, confidential information should be reported to the school as soon as possible.

Staff must not send school information to their personal email accounts.

Monitoring the use of personal devices

The school may use technology that detects and monitors the use of personal and other electronic or communication devices which are connected to or logged on to the school's wireless network or IT systems. By using a device on the school's network, staff and visitors agree to such detection and monitoring. The school's use of such technology is for the purpose of ensuring the security of its IT systems and tracking school information.

The information that the school may monitor includes, (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms, information uploaded or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content through school IT services or the school internet connection should report this to the school as soon as possible.

Security of staff personal devices

Any member of staff wishing to use their own device must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption. This should be more than a simple password protection.

Staff must ensure that personal devices are set to lock with encrypted passcodes to prevent unauthorised access. The device should be locked if they are unattended or set to auto-lock if it is inactive for a period of time.

Staff must never attempt to bypass any security controls in school systems or others' own devices.

Staff must ensure that appropriate security software is installed on their personal devices and must keep the software and security settings up-to-date.

Staff must ensure that passwords are kept securely and are not accessible to third parties. Automated log on processes to store passwords must not be used.

Support

The school takes no responsibility for supporting staff's own devices, nor does the school have a responsibility for conducting annual PAT testing of personal devices. However, the school will support staff in ensuring that they have appropriate levels of security in place.

Compliance, sanctions and disciplinary matters for staff

Non-compliance of this policy exposes both staff and the school to risks. If a breach of this policy occurs, the Staff Disciplinary & Misconduct policy will be applied.

Incidents and reporting

The school takes any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of the device should be reported to the school office in the first instance. Data protection incidents should be reported immediately to the school's Data Protection Officer.