



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn



Data Protection Policy

2025

Adopted: February 2019

Reviewed: November 2025

Next Review: November 2026



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

Contents

1. Aims.....	3
2. Legislation and guidance.....	3
3. Definitions.....	3
4. The data controller.....	5
5. Roles and responsibilities.....	5
6. Data Protection Principles	6
7. Collecting personal data.....	6
9. Subject access requests and other rights of individuals.....	9
10. Parental requests to see the educational record	11
11. Photographs and videos	11
12. Data protection by design and default	12
13. Data security and storage of records.....	13
14. Confidentiality.....	13
15. Disposal of records	14
16. Personal data breaches.....	16
17. Training	16
18. Links with other policies	16
Appendix 1: Personal data breach procedures	17



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

1. Aims

Barford St. Peter's C. of E. (VA) Primary School aims to ensure that all personal data collected about staff, pupils, parents, trustees, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

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

2. Legislation and guidance

This policy meets the requirements of 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)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

3. Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: <ul style="list-style-type: none">• Racial or ethnic origin• Political opinions• Religious or philosophical beliefs• Trade union membership• Genetics• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes• Health – physical or mental• Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

4. The data controller

Barford St. Peter's C. of E. (VA) Primary School processes personal data relating to parents, pupils, staff, governors, volunteers, visitors and others, and therefore is a data controller.

Barford St. Peter's C. of E. (VA) Primary School is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to all staff employed by Barford St. Peter's C. of E. (VA) Primary School, and to external organisations, volunteers and other individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing Board

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

5.2 Data Protection Officer

The data protection officer (DPO) is responsible for providing advice and guidance to the School in order to assist the School to implement this policy, monitor compliance with data protection law, and develop related policies and guidelines where applicable.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Our DPO is the School DPO Service and is contactable via admin3587@welearn365.com or alternatively;

School Data Protection Officer
Barford St. Peter's C. of E. (VA) Primary School
Church Street
Barford
CV35 8EW

5.3 Headteacher

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

5.4 Data Protection Champions

The School has nominated the following individuals as designated persons to be contacted internally in relation to all matters relating to data protection issues, and to make referrals, where necessary, to the Data Protection Officer:

Mary Baker who is contactable via; admin3587@welearn365.com or 01926 624244 and

Hannah Moore, the Data Protection Lead, who is contactable via admin3587@welearn365.com or 01926 624244

5.5 All staff

All members of staff are responsible for:



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

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

6. Data Protection Principles

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

Barford St. Peter's C. of E. (VA) Primary School has adopted the principles to underpin its Data Protection Policy: The principles require that all personal data shall be:

- (1) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
- (2) used for specified, explicit and legitimate purposes ('purpose limitation');
- (3) used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');
- (4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy');
- (5) kept no longer than is necessary ('storage limitation');
- (6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

Barford St. Peter's C. of E. (VA) Primary School shall only process personal data where it has one of 5 'lawful bases' (legal reasons) available to the School 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



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

- 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 (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

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

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

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

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

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

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

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 guidance set out in the Information and Records Management Society's toolkit for schools.

8. Sharing personal data

We will not normally share personal data with anyone else except as set out in the School's Privacy Notice. GDPR and the DPA 2018 also allow information to be shared where:

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

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

Where we transfer personal data internationally, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing, are sent either to the Data Protection Officer, a member of staff or a Governor/Trustee and include:

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

The DPO will send the subject access request to the Data Protection Lead. If staff receive a subject access request they must immediately forward it to the Designated Data Protection Lead, who will ensure that the DPO is informed.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the person should have parental



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

responsibility for the child, and 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 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils at our school will in general be granted without requiring the express permission of the pupil.

These are not fixed rules and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or 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 being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

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

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

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time, where processing is based on the consent of the pupil or parent
- 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
- Object to processing which has been justified on the basis of public task, official authority or



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

legitimate interests

- Challenge decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- 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 Data Protection Contact who will send it to the DPO for information purposes.

10. Parental requests to see the educational record

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

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Photographs and videos

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

The School 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.

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, unless we have consent, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Photographic Images Policy and Child Protection & Safeguarding Policy for more information on our use of photographs and videos.



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

12. Data protection by design and default

The School shall put measures in place to show that it has integrated data protection into all of its data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Consideration of whether a data protection impact assessment needs to be undertaken. The school will consider this if any of the following kinds of processing plan to be undertaken:
 - Use of systematic and extensive automated processing
 - Large scale processing of data, particularly where it involves special category or criminal offence data
 - Systematic monitoring of publicly accessible areas and any other form of surveillance
 - Processing of biometric or genetic data
 - Transfer of data outside of the European Economic Area
 - Profiling, evaluation or scoring
 - Automated decision making with legal or significant effects
 - Matching or combining datasets
 - Processing of data concerning vulnerable data subjects
 - Implementation of new technology or solutions
 - If processing would prevent a data subject from exercising a right or using a service or contract

On reviewing these criteria, if the school finds that the processing personal data presents a high risk to the rights and freedoms of individuals we will undertake a data protection impact assessment.

- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- 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



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

13. Data security and storage of records

The School 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:

- Portable electronic devices, such as laptops and hard drives that contain personal data are kept securely 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 must ensure passwords are hard for anyone else to guess by incorporating numbers and mixed case into it.
- Encryption software is used to protect all portable devices and removable media on which personal information is stored, 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 the Information Security 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 8)

14. Confidentiality

The School will provide all staff, students and volunteers with clear, unambiguous guidance regarding their legal and professional responsibilities in relation to confidentiality whilst they are at our school, and to provide clear expectations about how staff, students and volunteers should handle any information about children or their families.

When working in a school, students, volunteers and staff are placed in a position of trust by all stakeholders and there is an expectation that a professional approach will be used in all matters of confidentiality. As well as reading this policy, all volunteers, staff and students will be expected to sign a confidentiality agreement, before working in school.

Information Sharing:

- All information about individual children and/ or their families is strictly confidential and is only shared with staff or individuals who need to know based on the child's best interests.
- All safeguarding, medical and personal information about a child is held in a safe and secure place which can only be accessed by appropriate staff.
- All children have a right to the same level of confidentiality irrespective of gender, race, religion, culture, class, medical concerns and special educational needs.
- Staff must never discuss details of individual children, including their families, to any person without direct professional connection to and interest in the welfare and education of the individual concerned.



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

- Staff, students or volunteers must never discuss any aspect of an individual child or their behaviour or in the presence of another child.
- Governors should never ask for, or divulge, any details regarding individual children or their families to any person outside of a governing body meeting.
- Staff performance management should be carried out confidentially with the head teacher.
- Staff should follow the school procedure as set out in keeping children safe in education to report safeguarding concerns about children or their families. Safeguarding concerns should never be discussed with any member of staff other than the designated safeguarding leads.
- Class teachers and support staff may be aware of some confidential matters in order to support individual children and adults. These staff will respect the sensitivity of such cases and not divulge information to people unconnected professionally with the individual concerned.
- Staff should be aware of children in their care with medical needs. This information should not be publicly displayed (please see medical policy for more information).
- Governors must observe complete confidentiality, especially in relation to matters concerning individual staff, children or parents/carers. Although decisions reached at governors' meetings are normally made public through the minutes or otherwise, the discussions on which decisions are based are regarded as confidential. Governors should exercise the highest degree of prudence when discussion of potentially contentious issues arises outside of the governing body.

15. Disposal of records

Our School recognises that by efficiently managing our records, we will be able to comply with our legal and regulatory obligations, and to contribute to the effective overall management of our school. Maintaining good records helps us to provide the evidence needed to protect the legal rights and interests of our school, and for us to demonstrate our performance and accountability.

This section provides the framework through which we will effectively manage our records

15.1 Scope

This policy applies to all records created, received or maintained by permanent and temporary staff of the school in the course of carrying out its functions. Also, by any agents, contractors, consultants or third parties acting on behalf of the school.

Records are defined as all documents which facilitate the business carried out by the school and which are thereafter retained to provide evidence of transactions or activities. These records may be created, received or maintained in hard copy or electrical format e.g. paper documents, scanned documents, e-mails, audio and video recordings, text messages, notes of telephone and spreadsheets, Word Documents, presentations, etc.

15.2 Legislation and Guidance



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

This policy meets the requirements of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000 (FOIA 2000). It is based on the IRMS Toolkit For Schools, the Department of Education – Data Protection Toolkit for Schools, Department of Education – Annual Review of School Records and Safe Destruction Checklist, and guidance published by the Information Commissioner's Office (ICO) on the GDPR.

15.3 Responsibilities

- The Governing Body of the school/Academy Trust has a statutory responsibility to maintain the school's records and record keeping systems in accordance with the regulatory framework of the school.
- The Data Champion/School Business Manager will provide guidance on good records management practices within the school and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. The School Business Manager will monitor compliance with this policy by ensuring that the 'Annual Review of School Records Checklist' is completed at least annually.
- All members of Staff are responsible for ensuring that our school does not keep personal information for longer than is necessary for the purpose or purposes for which it was collected. Our school will manage and document its records disposal process in line with the guidance provided by the IRMS Toolkit for Schools.
- It is the responsibility of all members of the school to ensure that they:
 - Manage school records consistently in accordance with school's policies and procedures;
 - Properly document their actions and decisions;
 - Only share personal information appropriately and do not disclose it to an unauthorised third party;
 - Dispose of records securely

Staff who do not comply with this policy may face disciplinary action.

15.4 Safe Destruction of Records

All records containing personal information, or sensitive policy information will be made either unreadable or unreconstructable.

- Paper records should be shredded using a cross-cutting shredder
- CDs / DVDs / Floppy Disks should be cut into pieces
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded
- Hard Disks should be dismantled and sanded

Any other records will be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways.



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

Where an external provider is used, where possible, all records will be shredded on-site in the presence of an employee.

15.5 Freedom of Information Act 2000

The Freedom of Information Act 2000 requires us to maintain a list of records which have been destroyed and who authorised their destruction.

When destroying either a substantial amount of information or information which is of a particularly sensitive or important nature, members of staff should record at least:

- The information that has been destroyed
- The volume of the information that has been destroyed
- Who provided authorisation to destroy the information
- The date the information was destroyed

By following this guidance and completing the Annual Checklist, we will ensure that our school is compliant with the Data Protection rules and the Freedom of Information Act 2000.

16. Personal data breaches

The School shall take all reasonable steps to ensure that there are no personal data breaches.

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

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

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

17. Training

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

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

18. Links with other policies

This data protection policy is linked to our:

- Information Security Policy
- Photographic Images Policy



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

- Child Protection & Safeguarding Policy

Appendix 1: Personal data breach procedures

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it in accordance with this procedure.

When appropriate, the School will report the data breach to the ICO within 72 hours in accordance with the requirements of the GDPR.

1. Data protection breaches occur where personal data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully.
2. Examples of how a breach may occur include:
 - a. Theft of data or equipment on which data is stored;
 - b. Loss of data or equipment on which data is stored;
 - c. Inappropriate access controls allowing unauthorised use;
 - d. Accidental Loss;
 - e. Destruction of personal data;
 - f. Damage to personal data;
 - g. Equipment failure;
 - h. Unlawful disclosure of personal data to a third party;
 - i. Human error;
 - j. Unforeseen circumstances such as fire or flood;
 - k. Hacking attack; or
 - l. 'Blagging' offences where information is obtained by deceiving the organisation which holds it.
3. If any member of staff of the School, or Governor / Trustee, discovers that data has been lost, or



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

believes that there has been a breach of the data protection principles in the way that data is handled, you must immediately or no later than within 24 hours of first coming to notice, inform the School's Data Protection Contact.

4. Upon being notified, the School's Data Protection Contact will assess whether a breach of personal information has occurred, and the level of severity. If a breach has occurred but the risk of harm to any individual is low (for example, because no personal information has left the control of the School, then the School's Data Protection Contact will undertake an internal investigation to consider whether the Information Security Policy was followed, and whether any alterations need to be made to internal procedures as a result.
5. In all other cases, the incident must be notified to the Data Protection Officer immediately, who must follow the Information Commissioner's Office guidelines on notification and recording of the breach. The Data Protection Officer will provide advice and support on managing and responding to the data breach and advise whether they consider the incident to be reportable to the ICO. The priority must then be to close or contain the breach to mitigate / minimise the risks to those individuals affected by it.

All School staff and Governors / Trustees are expected to work in partnership with the Data Protection Contact and the Data Protection Officer in relation to the following matters

Notification of Breaches

Any member of staff or Governor / Trustee who becomes aware of a personal information breach should provide full details to the Data Protection Contact for the School within 24 hours of being made aware of the breach. A Data Breach Record Form must be completed and passed to the Data Protection Contact who will log it in the Incident Log. When completing the form details should be provided of the reporter's name, the date/time of the breach, the date/time of detecting the breach, and basic information about the type of breach and information about personal data concerned. Details of what has already been done to respond to the risks posed by the breach should also be included.

Containment and Recovery

The initial response is to investigate and contain the situation and a recovery plan including, damage limitation. You may need input from specialists such as IT, HR and legal and in some cases contact with external third parties.

- Seek assistance in the containment exercise. This could be isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment or simply changing any related access codes
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- As well as the physical recovery of equipment, this could involve the use of backup records to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Consider whether any individual affected by the data breach should be notified

Assessing the Risks

Levels of risk can be very different and vary on an individual breach of data security depending what is



Barford St. Peter's C.E. (V.A.) Primary School

Together we love; together we learn

lost/damaged/stolen. For example, if a case file is lost then risks are different depending on type of data and its sensitivity with potential adverse consequences for individuals. The Data Protection Contact should consider the following points:

- What type of data is involved?
- How sensitive is the data?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data has been affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to life?
- Loss of public confidence in the School?

All staff and Governors / Trustees should establish whether there is anything they can do to recover any losses and limit the damage the breach can cause.