Vicarage Primary School Retention Policy

Person responsible for the policy	**Sahara Shafik**
Date policy agreed by Governors	**June 2019**
Date to be next reviewed	**June 2020**

Signed by Chair of Governors:	**Signed by Head Teacher :**

The School recognizes that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records to provide evidence for protection the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

1. Scope of the policy

1.1 This policy applies to all records created, received or maintained by staff of the school in the course of carrying out its functions.

1.2 Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

1.3 A small percentage of the school's records will be selected for permanent preservation as part of the institution's archives and for historical research. This should be done in liaison with the County Archives Service.

2. Responsibility

2.1 The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Head of the School.

2.2 The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

2.3 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

3. Relationship with existing policies

This policy has been drawn up within the context of:

- Freedom of Information policy
- Data Protection policy
- Information Management Toolkit for schools IRMS

Signed: _____[Head of School]

Request for Information / Freedom of Information Act 2000 (FOIA)

1. Background

This guidance on Freedom of Information Act 2000 (FOIA) replaces the previous guidance sent to schools and educational establishments in November 2004.

This guidance contains up to date information on the Freedom of Information Act 2000 (FOIA) (this information has been obtained from the DFE and Information Commissioners websites). It is a legal right for any person to ask a school for access to information that it holds. The aim of the FOIA is to promote a culture of openness and accountability among public sector bodies and therefore improve public understanding of how public authorities (which include the governing bodies of maintained schools) carry out their duties, why they make the decisions they do and how they spend public money.

In principle, the FOIA enables people to access all information, including the reasoning behind decisions and policies, which do not fall under the DPA (Data Protection Act) or EIRs (Environmental Information Regulations).

For information:

- **Data Protection (DP) enquiries** (or subject access requests) are ones where the individual whom the information concerns asks to see what the school holds about them.
- **Environmental Information Regulations (EIR) enquiries** are ones which relate to air, water, land, natural sites, built environment, flora and fauna, and health, and any decisions and activities affecting any of these. These could therefore include enquiries about recycling, phone masts, school playing fields, car parking etc.
- **FOI enquiries** are concerned with all other information including the reasoning behind decisions and policies. All requests for information that are not DP or EIR are requests under the FOI Act.

Although FOI presumes openness, it recognises the need to protect sensitive information in certain circumstances and provides for exemptions.

Any request for information made in writing to a school since 1st January 2005 and which is considered 'non-routine' is a request under FOIA, EIRs, the DPA or a combination of any of them.

School governing bodies are responsible for ensuring that their school complies with the FOIA. The new legal presumption of openness since January 2005 makes it more important then ever that a school decides its policies and conducts its day-to-day operations in a way that stands up to public scrutiny. It should be noted that wilfully concealing, damaging or destroying information in order to avoid answering an enquiry is an offence and so a governing body, or any person who is employed by, or is an officer of, or is subject to the direction of the governing body (as the public authority) may be at risk of criminal proceedings.

The FOIA is overseen by the Information Commissioner. They also have responsibility for the Data Protection Act 1998 (DPA) (this act enables individuals to access information about themselves) and the Environmental Information Regulations 2004 (EIRs) (this act enables people to access environmental information).

2. Procedure on receiving an FOI request

A freedom of information checklist for action on receipt of a request for information is attached to this guidance.

If information is refused, record reasons for not doing so e.g. it is held by others, it is exempt, too costly, not in the public interest. Further information about Freedom of Information can be obtained from: http://www.ico.gov.uk/for_organisations/freedom_of_information.aspx

3. Charging under the FOI Act

There is a limit to the costs for the information being provided. If that cost exceeds £450 limit for schools, you can refuse the request:

To estimate whether the costs will be over the limit you can only include the following costs:

- determining whether your school holds the information;
- locating the information, or a document which may contain it;
- retrieving the information, or a document which may contain it; and

- extracting the information from a document containing it.

For the purpose of the estimate, you should cost the time taken on these activities at £25 per person per hour regardless of actual cost.

Your estimate cannot include the following costs:

- considering whether the information is exempt;
- redacting (removing) exempt information; or
- copying and sending information.

The guidance 'using the fees regulations' gives detailed advice on how to estimate costs and apply – this can be found on www.ico.gov.uk/for_organisations/freedom_of_information/information_request/costs.aspx

Charging fees – The 'Fees Regulations' accompanying the Act sets out the fees that can be charged for requests and the limits to the costs that may be incurred. This guidance can be found on: www.ico.gov.uk/for_organisations/freedom_of_information/information_request/costs.aspx
If the cost of answering the request would be below the appropriate limit then you can only charge a fee to recover the costs of:

- contacting the requestor to inform them that the information is held;
- communicating the information to the requestor (e.g. photocopying, printing and postage); and
- putting the information into the format specified by the requestor.

These costs are often referred to as 'disbursements'.

You cannot charge for:

- staff time;
- removing exempt information from the information you are providing; or
- use of contractors or specialist staff.

If you intend to charge a fee you must send the requestor a fees notice within the normal 20 working days. The requestor then has three months in which to pay the fee and you do not have to provide the information until the fee is

received. The time from when the fees notice is issued until the fee is received does not count towards the 20 day limit.

The guidance on 'charging a fee' explains what is involved in issuing a fees notice – this guidance can be found on: www.ico.gov.uk/for_organisations/freedom_of_information/information_request/costs.aspx

If you estimate the cost of answering the request to exceed the appropriate limit, you are not obliged to provide the information but you can if you wish offer to provide it in return for a fee representing the cost of answering the request. In such a case the fee could include the cost of staff time (at £25 per hour) as well as the actual expenditure incurred. The guidance on 'using the fees regulations' explains this.

4. Retention Policy

Schools must ensure that they all have a working retentionpolicy which has been agreed by the Governing Body and ensure that all staff are aware of it. (Policy attached)

You must ensure:-

- staff are aware of the rights of people to obtain information under the Act;
- a retention schedule is established, in line with the enclosed retention guidelines;
- there are procedures for keeping records of requests for information.
- all requests are recorded and dated when a request is made and the date when information is given. Remember there is a time limit of 20 working (school) days;
- a copy of the information provided is retained.

Schools must ensure records are kept for set periods of time according to the record type. The attached document "Retention Guidelines for Schools" produced by the Information Management Toolkit for Schools will assist schools with ascertaining the appropriate retention period for the record.

5. Data Protection Public Register

The school is registered on the Data Protection Public Register. If an enquirer is not happy with the outcome of their request or decision they are advised to follow the school's complaint procedures. Once this has been exhausted, the enquirer can then appeal to the Information Commissioner, for this purpose the following address should be provided:

The Information Commissioner, FOI Compliance Team (complaints), Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

FREEDOM OF INFORMATION - CHECKLIST FOR ACTION ON RECEIPT OF A REQUEST FOR INFORMATION

Task to be undertaken		Completed	Not Required
Decide whether the request is a request Under:	DATA PROTECTION ACT		
	ENVIRONMENTAL INFORMATION REGULATIONS		
	FREEDOM OF INFORMATION ACT		
Decide whether the school holds the information or whether the request should be transferred to another body if the information is held by them.			
Provide the information if it has already been made public.			
Inform the enquirer if the information is not held.			
Consider whether a third party's interests might be affected by disclosure and if so consult them.			
Consider whether any exemptions apply and whether they			

are absolute or qualified		
Carry out a public interest test to decide if applying the qualified exemption outweighs the public interest in disclosing the information.		
Decide whether the estimated cost of complying with the request will exceed the appropriate limit – see paragraph 3 charging.		
If a request is made for a document that contains exempt personal information ensure that the personal information is removed by applying the appropriate editing procedures.		
Consider whether the request is vexatious or repeated.		

Remember

Schools are under a duty to provide advice and assistance to anyone requesting information.

The enquirer is entitled to be told whether the school holds the information (the duty to confirm or deny) except where certain exemptions apply.

A well-managed records and management information system is essential to help schools to meet requests.

Requests should be dealt with within 20 working days excluding school holidays.

Wilfully concealing, damaging or destroying information in order to avoid answering an enquiry is an offence. A valid FOI request should be in writing, state the enquirer's name and correspondence address and describe the information requested.

Expressions of dissatisfaction should be handled through the school's existing complaints procedure.

Vicarage Primary School Data Protection Policy

Person responsible for the policy	**Sahara Shafik**
Date policy agreed by Governors	**June 2019**
Date to be next reviewed	**June 2020**

Signed by Chair of Governors:	**Signed by Head Teacher :**

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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 GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

3. 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 ▪ Religious or philosophical beliefs ▪ Trade union membership ▪ Genetics ▪ 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 electronic or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

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

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

5. Roles and responsibilities

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

5.1 Governing board

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

5.2 Data protection officer

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

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

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

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

Our DPO is **Louise Malina** and is contactable via **NPW 020 8249 6977**

5.3 Head teacher

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

5.4 All staff

Staff are responsible for:

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

6. Data protection principles

- The GDPR is based on data protection principles that our school must comply with.
- The principles say that personal data must be:
- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

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

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

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

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

7.2 Limitation, minimisation and accuracy

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

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

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

When staff no longer needs the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Retention Policy.

8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

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

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

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

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

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

- Name of individual
- Correspondence address
- Contact number and email address

Details of the information requested

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

9.2 Children and subject access requests

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

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is

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

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or 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 takes into account administrative costs.

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

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

9.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time

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

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

10. Parental requests to see the educational record

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

11. CCTV

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

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

Any enquiries about the CCTV system should be directed to Head Teacher.

12. Photographs and videos

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

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

Uses may include:

- Within school on notice boards, displays, school magazines, brochures, and newsletters
- 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 and safeguarding policy/photography policy/other relevant policy] for more information on our use of photographs and videos.

13. Data protection by design and default

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

- Appointing a suitably qualified 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)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment see our online safety 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)

15. Disposal of records

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

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

16. Personal data breaches

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

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

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

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

17. Training

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

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

18. 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. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

19. Links with other policies

This data protection policy is linked to our:

Freedom of Information Act

Retention Policy

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

- The DPO will alert the head teacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation

- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

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

- The DPO will document the decision (either way); in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on a designated software solution.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

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

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on a designated software solution.

The DPO and head teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach that you might want to consider 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

Retention Guidelines

1. The purpose of the retention guidelines

Under the Freedom of Act 2000, schools are required to maintain a retention schedule listing the record series which the school creates in the course of its business. The retention schedule lays down the length of time which record needs to be retained and the action which should be taken when it is of no further administrative use. The retention schedule lays down the basis for normal processing under both the Data Protection Act 1998 and the Freedom of Information Act 2000.

Members of staff are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

The retention schedule refers to record series regardless of the media in which they are stored.

2. Benefits of a retention schedule

There are a number of benefits which arise from the use of a complete retention schedule:

Managing records against the retention schedule is deemed to be "normal processing" under Data Protection Act 1198 and the Freedom of Information Act 2000. Members of staff should be aware that once a Freedom of Information request is received or a legal hold imposed then records disposal relating to the request or legal hold must be stopped.

Members of staff can be confident about safe disposal information at the appropriate time.

Information which is subject to Freedom of Information and Data Protection legislation will be available when required. The school is not maintaining and sorting information unnecessarily.

3. Maintaining and amending the retention schedule

Where appropriate the retention schedule should be reviewed and amended to include any new record series created and remove any obsolete record series.

Version 5

This retention schedule contains recommended retention periods for the different records series created and maintained by schools in the course of their business. The schedule refers to all information regardless of the media in which it is stored.

Some of the retention periods are governed by statute. Others are guidelines following best practise. Every effort has been made to ensure that these retention periods are compliant with the requirements of the Data Protection Act 1998 and the Freedom of Information Act 2000.

Managing record series using these retention guidelines will be deemed to be "normal processing" under the legislation mentioned above. If record series are to be kept for longer or shorter periods that laid out in this document the reasons for this need to be documented.

This schedule should be reviewed on a regular basis.

This document is a guideline only and liability is the liability of the end user and not of the IRMS. Individual organisations should seek the appropriate legal advice and senior management approval.

These retention guidelines are free for use to schools. Questions will only be dealt with if they are submitted by IRMS members. Please complete the form on the webpage remembering to include your IRMS membership number.

Further details about the benefits of IRMS membership can be found at:
http://www.irms.org.uk/join

Using the Retention Schedule

The Retention Schedule is divided into five sections:

1. Management of the School
2. Human Resources
3. Financial Management of the School
4. Property Management
5. Pupil Management
6. Curriculum Management
7. Extra-Curricular Activities
8. Central Government and Local Authority

There are sub headings under each section to help guide you to the retention period you are looking for. Each entry has a unique reference number. If you are sending a query to the IRMS about an individual retention period, please ensure that you have quoted the unique reference number.

The IRMS will only deal with queries relating to the retention schedule from IRMS members.