Data Protection Policy

Responsibility: Portsmouth Catholic Diocese

Reviewed by: Sandra Barry, Head teacher

This Review: May 2018

Next Review Due: May 2019

Cycle: Yearly

Ratified by Full Governing Body on:

Signed:

Chair of Governors Hans Daems

Data Protection Policy

The school collects and uses personal information (referred to in the General Data Protection Regulation (GDPR) as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.
The school is the Data Controller, of the personal data that it collects and receives for these purposes.

The school has a Data Protection Officer, who may be contacted via the school office.

The school issues Privacy Notices (also known as a Fair Processing Notices) to all pupils/parents and staff. These summarise the personal information held about pupils and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data

Purpose
This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information/ data?
Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles

The GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes)

3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive;

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

5. Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6. Personal data shall be processed in a manner that ensures appropriate security of the personal

Duties

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

Commitment

The school is committed to maintaining the principles and duties in the GDPR at all times. Therefore the school will:

- Inform individuals of the identity and contact details of the data controller

- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information
- Inform individuals of their data subject rights
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests)
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
- Ensure that all staff and governors are aware of and understand these policies and procedures.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Data Protection Officer, Head teacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact Martin Tubbs, Data Protection Officer on 01628 796945 or by e-mail, martin.tubbs@rbwm.gov.uk

Appendices

1. Privacy Notice (Published on website)
2. Information for Staff and Governors
3. Staff agreement (to be filed in personnel records)
4. Checklist for Obtaining Consent
5. Consent template form
6. Information Audit
7. HCC Retention Schedule
8. Subject Access Request Checklist
9. Subject Access Request Guidance
10. Data Protection Impact Assessment Guidance and Form
11. Data Breach Initial Reporting Form

Appendix 1

Privacy Notice (How we use personal information)

Why do we collect and use personal information?

We collect and use personal information:

- to fulfil statutory responsibilities, legislative duties or duty of care
- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services and how well our school is doing
- Statistical forecasting and planning
- to comply with the law regarding data sharing
- to comply with our Safeguarding procedures
- for the protection of vital interests
- for the provision of health and wellbeing
- for the performance of a contract

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

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as religion, ethnicity, language, nationality, country of birth and free school meal eligibility)
- Family and contact details
- Attendance information (such as sessions attended, number of absences and absence reasons) and exclusions
- Assessment information
- Modes of travel
- Relevant medical, special educational needs and behavioural information

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

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

Collecting personal information

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

Storing personal data

We hold pupil data in accordance with our retention schedule *(see appendix 7)*

Who do we share pupil information with?
We routinely share pupil information with:

- schools that the pupils attend after leaving us
- our local authority
- the Department for Education (DfE)
- School health

Why we share pupil information
We do not share personal information with anyone without consent unless the law and our policies allow us to do so.
We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

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

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

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

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

To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

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

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

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

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data.

Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

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

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

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

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

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

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

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

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

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

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

Martin Tubbs, Data Protection Officer on 01628 796945 or by e-mail, martin.tubbs@rbwm.gov.uk

Appendix 2

St Mary's Catholic Primary School

Information for Staff and Governors

Reforms to data protection will come into force in May 2018. The General Data Protection Regulation (GDPR) will determine how personal data is processed and kept safe, and the legal rights people have in relation to their own data.

What is the General Data Protection Regulation?

The General Data Protection Regulation (GDPR) is a piece of EU-wide legislation which will determine how people's personal data **is processed and kept safe, and the legal rights individuals have in relation to their own data. It will apply from 25 May 2018 to organisations that process or handle personal data, including schools.**

It's similar to the Data Protection Act (DPA) 1998 in many ways. Most of the differences involve the GDPR building on or strengthening the principles of the DPA.
The document setting out the full regulation is here:

General Data Protection Regulation, Council of the EU (Adobe pdf file)http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

The UK government has confirmed that the UK will be implementing the GDPR despite its intention to leave the EU.

How the ICO will be supporting the implementation of the GDPR, ICO, 31 October 2016https://iconewsblog.wordpress.com/2016/10/31/how-the-ico-will-be-supporting-the-implementation-of-the-gdpr/

What will be different?

The Information Commissioner's Office (ICO), **the organisation that upholds information rights in the UK, has explained which key areas of data protection schools may have to change their practices in once the GDPR is in place.**

Data protection for the education sector webinar, ICOhttps://ico.org.uk/about-the-ico/news-and-events/events-and-webinars/data-protection-for-the-education-sector-webinar/

Privacy notices

The GDPR is more detailed on what you must include in your privacy notice. You still need to say who you are, why you process information and what you do with it, but now you must also include items such as your legal basis for processing, the individual's right to make a complaint to the supervisory authority and other rights in relation to access and correcting inaccurate data.

All privacy notices should be in clear and plain language, but particularly those that refer to children's data – so that a child can easily understand.

Subject access requests

Currently, you have 40 days to comply with a subject access request and in some circumstances you can charge for the cost of complying.
Under the GDPR, you won't be able to charge in most cases, and normally you'll have just a **month to comply.**

Consent

The GDPR brings in stricter rules around consent.

Consent for processing someone's personal data must be freely given, specific, informed and unambiguous, and a positive affirmation of the individual's agreement. **For example, this may be relevant for any contact preferences you hold for parents and alumni for school fundraising purposes.**

Protections for children

For the first time, the GDPR will bring in special protection for children's personal data, though **only in the context of commercial internet services such as social networking.**
You will need to consider whether parental/guardian consent is required for the data processing you carry out with regards to things such as using apps in the classroom.

Data breaches

The ICO must now be notified within 72 hours of data breaches where an individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach.

Data protection impact assessments

It's currently good practice to carry out a privacy impact assessment when your school is **considering using data in new and innovative ways, or implementing new technology to monitor pupils in some way.**
This will become a legal requirement in some circumstances under the GDPR. The ICO suggests, for example, that you might do this where you've considered implementing a new web monitoring system in the classroom or sharing data with a local troubled families initiative. We've got another article with more detail on what they are, and when you might need to conduct one.

Data protection officers

You can currently choose whether you want a designated data protection officer in your school. Under the GDPR, all public authorities must designate a data protection officer to take responsibility for data protection compliance. This means that many schools will need to put this in place for the first time. Consider where this role will sit within your organisation's str**ucture and governance arrangements.**
You can read more about the role of a data protection officer in another article.

Demonstrating compliance

Organisations will have to be able to demonstrate how they comply with the new law. It's **important that schools are committed at the highest level to putting the relevant policies and procedures in place.**

To demonstrate compliance, we will:

- **Appoint a data protection officer (M Tubbs) to be the point of contact for all data protection queries and subject access requests and to implement, monitor data protection in school and arrange training.**
- **Put in place appropriate technical and organisational measures**
- Keep records on data processing activities (e.g. records of what data you've shared with **which organisations, and how you made the decision to do so)**
- **Undertake data protection impact assessments where necessary**
- **Obtain consent for the collection of any data for any reason outside of the legal bases** stated on the school's privacy statement.

Fines

Currently the maximum fine for breaching the Data Protection Act is £500,000.
This will increase to 20 million euros under the GDPR, although the regulation does state that the fine must be "proportionate", and each member state may lay down its own rules on whether and to what extent fines may be imposed.

Appendix *3*

Data Protection and Confidentiality Statement

Staff and Governors

I confirm that I have read the Data Protection and Confidentiality Policies and adhere to the clauses within them with regard to Confidentiality and Data Protection.

For the purposes of this document, Personal data includes all personal and sensitive data for children and staff.

In particular I undertake to follow the procedures below to ensure that personal data is secure:

- All personal data held must be accurate, relevant and secure.
- Explicit consent must be sought for collecting and sharing data for purposes other than for a legal basis, such as using photographs or completing surveys.
- Documents which hold personal data will be kept secure. If documents are removed from the school for an approved purpose they will be carried in a secure briefcase (paper files) or on an encrypted data stick (electronic)
- Passwords will be kept confidential and changed regularly
- Any loss or potential loss of data or breaches of confidentiality must be reported immediately to the Data Protection Officer (DPO)
- Children's personal data will not be displayed in the school. First names only can be used on work, photographs must not be matched with names.
- For the purposes of taking books home for marking, books will be labelled with first names only. Children will be advised not to use photographs on their homework books.
- Passwords for the computer system and Sims must not be on display
- Computers must be locked or shut down when leaving the room.
- Children's personal information should never be displayed on the interactive television. (Dinner register during registration only are exceptions.)
- Staff will not enter personal data on any computer or online system without informing the Data Protection Officer, completing a Privacy Impact Assessment and Information sharing agreement.
- Personal data will not be held on personal computers at home.
- Prior to 25th May 2018 all staff will ensure that they possess no personal data on home computers, non encrypted data sticks or in paper form.
- Emails containing personal data will only be sent when there is no other option and only to other e-mail addresses known to be secure and accessed only by the intended recipient.

Signed ……

Date ……

Examples of Data Breaches include but are not limited to:

- Sending e-mails / letters to the wrong address
- Leaving files containing confidential information in a public place
- Staff removing information from school which they are not permitted to take (potential criminal offence)
- Failing to keep personal details of separated parents confidential
- Sending confidential information by unsecured post which goes missing
- Accessing confidential information online which can be observed by pupils / third parties

Appendix 4

Checklist for obtaining consent under the GDPR

Action	✓
Asking for consent	
We have checked that consent is the most appropriate lawful basis for processing	
We have made the request for consent prominent and separate from other terms and conditions	
We ask people to positively opt in	
We don't use pre-ticked boxes, or any other type of consent by default	
We use clear, plain language that is easy to understand	
We specify why we want the data and what we're going to do with it	
We give granular options to consent to independent processing operations	
We have named our organisation and any third parties	
We tell individuals they can withdraw their consent	
We ensure that the individual can refuse to consent without detriment	
We don't make consent a precondition of a service	
Recording consent	
We keep a record of when and how we got consent from the individual	
We keep a record of exactly what they were told at the time	
Managing consent on an ongoing basis	
We regularly review consents to check that the relationship, the processing and the purposes have not changed	
We have processes in place to refresh consent at appropriate intervals, including any parental consents	
We make it easy for individuals to withdraw their consent at any time, and publicise how to do so	
We act on withdrawals of consent as soon as we can	
We don't penalise individuals who wish to withdraw consent	

Appendix 5

St Mary's Catholic Primary School

Cookham Road
Maidenhead
SL6 7EG
t: 01628 622570
e: office@stmarys-maidenhead.org.uk
w: www.stmarys-maidenhead.org.uk
Headteacher: Mrs. S. Barry

Date:

Dear Parent/Carer,

At St Mary's School we sometimes take photographs of pupils. We use these photos on the school's website and on display boards around school. Occasionally these may, with your consent, be used in press releases.

We would like your consent to take photos of your child, and use them in the ways described above. If you're not happy for us to do this, that's no problem – we will accommodate your preferences.

Please tick the relevant box(es) below and return this form to school.

I am happy for the school to take photographs of my child. ☐

I am happy for photos of my child to be used on the school website. ☐

I am happy for photos of my child to be used in internal displays. ☐

I am happy for photos of my child to be used in media photographs (unnamed) ☐

I am **NOT** happy for the school to take or use photos of my child **other** than evidence in class books/altar books that are for class/assessment use only. ☐

If you change your mind at any time, you can let us know by emailing office@stmarys-maidenhead.org.uk or calling the school on 01628 622570 or just popping in to the school office.

Without your consent we cannot contact you by email. Please tick the box to confirm that you are happy to receive email communication from the school including, receiving the newsletter and other school related information. ☐

If you have any other questions, please get in touch.

Why are we asking for your consent again?

You may be aware that there are new data protection rules coming in from May. To ensure we are meeting the new requirements, we need to re-seek your consent to take and use photos of your child and to communicate with you via email. We really value using photos of pupils, to be able to showcase what pupils do in school and show what life at our school is like to others, so we would appreciate you taking the time to give consent again.

Child's name

Parent/Carer's signature: _____

Date:

Appendix 6

DATA MAPPING

PD = Personal Data SC = Special Category Data.

Personal Data: includes identification of individuals from identifiers – NI numbers, location data

•**Special Category Data:** (was sensitive personal data) now includes biometric data (e.g. fingerprint scanning).

For **personal** data schools are likely to use the following legal basis:

•Performance of a contract with data subject (e.g. for staff data).

•Compliance with a legal obligation (e.g. legally obliged to keep parents contact details).

•Protection of vital interests. (e.g. child protection)

•Necessary for performance of public interest tasks. (awaiting guidance) – educating pupils on behalf of DFE

•Consent (only rely on if nothing else applies).

Can only use **Special Category Data (SCD)** if one of following conditions apply: (these are conditions most relevant to schools)

•Necessary and authorised by law for employment obligations.

•Protect vital interests and consent not feasible.

•Necessary for establishing, exercising or defence of legal rights.

•Substantial public interest (still subject to change in DP Bill) Requires organisation to have a DP policy**.**

•Explicit consent.

Data Subject	Description of Data*	Type of Data		How is it collected	What is it used for?	What is the legal basis for using it?	What is the legal basis for using it?	Where is it stored?	Does it leave the school?	Who is it shared with?	Who can access it	How long is data kept?
		PD	SC									

Appendix 7

School Records Retention Schedule for St Mary's Catholic Primary School

Table of contents

1. About the schedule

The school records retention schedule has been drawn up in response to requests for assistance on recordkeeping from Hampshire schools. This guidance is intended for maintained schools, not academies.

The schedule contains guidelines on how long to keep records created and maintained by schools in the course of their business, and how those records should be disposed of at the end of their administrative life. Records may be held in any format, including paper, electronic (including databases), microform and audio-visual.

Disposing of records at the right time in accordance with clearly established policies will help schools to ensure they meet recordkeeping requirements set out in the Data Protection Act (DPA) 1998 and Freedom of Information Act (FOI) 2000, particularly the Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the FOI.

2. How the schedule is arranged

The schedule is arranged by type of record. The 'Retention Period' specifies how long the record should be kept and the 'Final Action' describes how they should be disposed of. If records need to be kept for legal reasons, the relevant statute is cited in the 'Legal Status' column. If no legal status is given, the retention period is based on best practice, considering administrative, audit and legal requirements.

The column headed 'DPA applies?' indicates whether records contain personal information. Such records are subject to the Data Protection Act 1998 and should be stored securely, and safe from unauthorised access.

This schedule may need to be adapted to suit the requirements of your particular school. Hampshire County Council's Records Management Service can offer advice as needed; contact details are given below.

3. What to do at the end of the retention period

Note re disposal: You may be aware of the Independent Inquiry into Child Sexual

Abuse (IICSA). While this inquiry is being carried out, schools have been asked to retain records relating to child protection until further notice.

For more information, please see the letter from the Chair of the Inquiry to local authorities on the IICSA website: https://www.iicsa.org.uk/key-documents/82/view/letter-to-local-authority-ceos.pdf

Destroy

Where records have been identified for destruction they should be disposed of in an appropriate way:

- All paper records containing personal information, or sensitive policy information, should be disposed of as confidential waste. Contact County Supplies for advice on the availability of confidential shredding in your area (tel. 01962 826999). *Yellow Pages* also lists local commercial shredding services.

- All confidential electronic records should be deleted securely from electronic systems, including databases. N.B. Simply deleting data is unlikely to be sufficient, as records that are no longer visible may still be recoverable; remember that back-ups will need to be destroyed too..

- Non-confidential records should be bundled up and disposed of to a waste paper merchant, or recycled in other appropriate ways.

It is recommended that schools maintain lists of records which have been destroyed, giving file references, titles, dates of destruction and name of authorising officer. An Excel spreadsheet or other database format could be used for this.

Review

Records are marked for review in cases where there is no longer a statutory or financial requirement for retention but where the decision to destroy is not clear cut.

Assess the record's continuing administrative or historical worth. Consider keeping files that relate to:

- Major events or important developments in the life of the school
- Major policies and / or long-term strategies
- Claims (or possible claims) for compensation

You will likely dispose of:

- Routine papers and correspondence
- Papers that refer to events of short-term relevance and minor interest.

4. Storage, display and handling of school records

These general guidelines on the storage, display and handling of archives should be followed to help ensure the long-term preservation of school records regarded as historically significant.

Keep documents out of direct sunlight and avoid extremes of temperature and humidity:

- For paper records a temperature of 13-20°C is ideal, with a relative humidity (RH) of between 35-60%. (RH is read by a hygrometer[1].)
- Audio tapes require cool, dry conditions (40-60% RH, 13-16°C).
- Try not to store records near radiators where the air will be too hot and dry.
- Records which do not need to be referred to regularly should ideally be stored in a room where staff are not required to work.

Ensure that storage is on well-ventilated shelving and that storage areas are kept clean

- Don't pack records together too tightly as lack of air flow encourages mould. Mould-affected items should be separated out.
- Ventilate storage rooms well.
- Keep storage areas clean, as dust and dirt can accelerate decay and encourage pests.

Use good quality storage materials

- 'Archival quality' packaging materials are free of acids and other chemicals which will make paper brittle and cause inks to fade. They are available commercially, and although expensive, need only be used for those items which are to be kept permanently. Names and addresses of some commercial suppliers are given at the end of this guidance note.
- If possible, use archive-quality boxes, made from rigid container board with non-rusting staples and well-fitting lids. Strong cardboard boxes lined with acid-free paper, and with a lid to keep out dust, are a cheaper alternative.
- Written records can be protected by wrapping them in archival quality paper or card. Photographs should be placed in clear polyester sleeves if kept loose, or mounted using photo corners if they are in an album. Alternatively, use good quality envelopes with the gummed flap removed, and card folders or large sheets of cartridge paper folded to size.
- For all records, use good quality fastenings, e.g. wide cotton tape, brass staples, brass paper clips, and plastic treasury tags. Number documents or pages, if necessary, in pencil only.

Use good inks and papers:

- When you are creating paper records which you know will need to be kept long term, use good quality permanent ink and acid-free paper if you can, and avoid ball point pens, particularly blue and red, which fade quickly.

Avoid the following, all of which are detrimental to your archives if they are to be kept long-term:

- steel pins and paperclips; plastic bags; photo albums using cheap PVC overlays and adhesives to secure photos; PVC wallets; sellotape; pink document tape; elastic bands.

Displaying and handling records always puts them at risk

- Displaying potentially valuable items leaves them open to the risk of vandalism or theft. Look after your archives at all times and display them only in lockable showcases. (HALS is able to lend lockable showcases free of charge, subject to availability.)
- Inks and colours can fade if exhibited in bright light for too long, and the spines and bindings of volumes can be weakened by prolonged use or opening in the same position. Aim therefore to display records away from direct heat and sunlight. Support volumes,

[1] Inexpensive, easy-to-use, hand-held electronic hygrometers can be bought from Preservation Equipment ltd., Vinces Road, Diss, Norfolk, IP22 4HQ (tel. 01379 647400) www.preservationequipment.com

ideally on cushions, so that they are not open too wide, using strips of clear polyester to secure pages if necessary. Never use sellotape, drawing pins or metal staples to fasten documents being displayed.

- If records are used in the classroom, keep control of them. Make sure you know what you have and where it should be when not in use. Ask those who borrow the records to handle them with care, to use only pencil when making notes from them, and to supervise their use at all times. Photocopied extracts from the records could be used as a substitute to protect originals from over-handling.

Archival-quality paper, boxes and packaging materials can be purchased from:

Conservation Resources (UK) Ltd. www.conservationresources.com
Unit 2, Ashville Way, off Watlington Road, Cowley, Oxford, OX4 6TU Tel. 01865 747755

Preservation Equipment Ltd. www.preservationequipment.com
Vinces Road, Diss, Norfolk, IP22 4HQ Tel. 01379 647400

Conservation By Design Ltd. www.conservation-by-design.co.uk
2 Wolseley Road, Kempston, Bedford, Conservation By Design, MK42 7AD

No.	Basic File Description	DPA applies?	Statutory Provisions	Retention Period	Final Action	Notes
1.0	**School Governors**					
1.1	Instruments of government, including Articles of Association	No		Permanent	**Permanent** Retain in school while current	
1.2	Records for all full governing body, committee and panel meetings, including: a) agendas b) any report, statutory policy (including Admissions Policy) or other paper	Yes*	School Governance (England) Regulations (2013)	Permanent	**Permanent, or as below** Single copy of signed minutes, agenda and papers: retain in school for 6 years from date of meeting. Inspection copies: retain in school for	*If meeting deals with confidential staff issues

	considered at governing body meeting c) signed minutes				current year + 3 then destroy as confidential waste or delete securely Additional copies: destroy as confidential waste or delete securely from electronic systems	
1.3	Governors application forms - successful candidates	Yes		End of term of office + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
1.4	Governors application forms - unsuccessful candidates	Yes		Date of election + 6 months	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
1.5	Governor election voting forms	Yes		Date of election + 6 months	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
1.6	Governors - registers and declarations of pecuniary interests	Yes		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
1.7	Trusts and endowments managed by the governing body	No		Permanent	**Permanent** Retain in school whilst operationally required, then transfer to HALS	
1.8	Action plans created and / or	No		Life of action plan + 3	**Destroy** Destroy as	

	administered by the governing body			years	confidential waste or delete securely from electronic systems	
1.9	Records relating to complaints dealt with by the governing body	Yes		Date of resolution of complaint + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems*	*It may be appropriate to review for further retention in the case of contentious disputes
1.10	Annual parents' meetings			Permanent	**Permanent, or as below** Retain in school for 6 years from date of meeting All other records: destroy as confidential waste or delete securely from electronic systems	

2.0	**Management and Administration**					
2.1	Log books of activity in the school, maintained by teachers	Yes[2]		Permanent	**Permanent** Retain in school whilst operationally required.	
2.2	Head teacher's official diary	Yes[1]		Current academic year + 3 years	**Destroy** Delete securely or destroy as confidential waste.	

[2] Since 1 January 2005 subject access has been permitted into unstructured filing systems, including log books and other records created within the school, containing details about the activities of individual pupils. As such members of staff are subject to the Data Protection Act 1998.

2.3	Minutes of the senior management team and other internal administrative bodies	Yes[1]		Permanent	**Permanent, or as below** Retain in school for 5 years from date of meeting. All other records: destroy as confidential waste or delete securely from electronic systems	
2.4	Reports made by the head teacher or the management team	Yes[1]		Retain in school for date of report + 3 years	**Permanent**	
2.5	Correspondence and general filing created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes[1]		Closure of file + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
2.6	Professional development plans	Yes		Closure of file + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
2.7	School development plans	No		Retain in school for closure of file + 6 years	**Transfer to archive**	
2.8	Employers' liability certificate	No		Permanent while school is operational	**Destroy** Destroy as confidential waste or delete securely from electronic systems once school closes	
2.9	School brochure/prospectus	No		Retain in school for current academic year + 3 years	**Transfer to archive**	

2.10	Circulars to staff and pupils	No		Current academic year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
2.11	Newsletters to parents	No		Retain in school for current academic year + 3 years	**Transfer to archive**	
2.12	Visitors' books and signing in sheets	Yes		Current academic year + 6 years	**Destroy** Destroy as confidential waste	

3.0	**LEA (Local Education Authority)**					
3.1	Secondary transfer sheets (primary)	Yes		Current academic year + 2 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
3.2	Attendance returns	Yes		Current academic year + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
3.3	Circulars from the LEA	No		Whilst operationally required	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

4.0	**DfE (Department for Education)**					
4.1	HMI reports	No		Permanent	**Permanent** Retain in school whilst operationally required.	These are no longer produced

4.2	OFSTED reports	No		Retain in school while current; replace former report with any new inspection report	**Permanent**	Reports should be available on the OFSTED website. Retain at least two previous reports if not available online.
4.3	OFSTED-related papers	No		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
4.4	Returns to the DfE	No		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
4.5	Circulars from the DfE	No		Whilst operationally required	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
4.6	School census returns	Yes	Education (School Performance Information) (England) Regulations 2007	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

5.0	**Pupils**					
5.1	Records relating to the creation and implementation of the school's Admissions Policy	No	School Admissions Code (2014)	Retain in school for life of the policy + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.2	Admission forms: unsuccessful or withdrawn applications (including supplementary information e.g. proof of address, religion, medical conditions etc.)	Yes	School Admissions Code (2014)	a) If no appeal, 1 year from receipt b) If appealed, 1 year from resolution of case*	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*Records relating to appeals retained by Appeals Panel for 22 years from date of birth of pupil
5.3	Admission forms: successful applications	Yes	School Admissions Code (2014)	Date of admission + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Ensure that supplementary information e.g. proof of address, religion, medical conditions is added to the pupil's file
5.4	Admission registers	Yes	Education (Pupil Registration) (England) Regulations 2006	Retain in school until date of last entry in the book (or file) + 3 years	**Permanent**	If held electronically, a printout should be made at least **annually**. Any corrections made to electronic data should be clearly shown in the printout.
5.5	Attendance registers	Yes	Education (Pupil Registration) (England) Regulations 2006	Date of register + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

5.6	Pupil absence letters / leave forms / correspondence relating to authorised absence	Yes		Date of absence + 2 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.7	Telephone message books for recording absences (sickness) or changes to pick up arrangements, etc.	Yes		Current year + 6 years from last entry in book	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.8	Child protection files • **Primary**	Yes	DfE 'Keeping Children Safe in Education' (2016), Annex B, p.61	Retain while the pupil remains at the primary school*	Follow guidelines in 5.13 for pupils transferring to another school	*CP information must be kept separate from the main pupil file. Where children leave the school or college ensure their child protection file is transferred to the new school or college as soon as possible. This should be transferred separately from the main pupil file, ensuring secure transit. Confirmation of receipt should be obtained.

5.9	Pupil's educational record (pupil file) **Pupils with Special Educational Needs (SEN)** • **Primary**	Yes	Retain while pupil remains at the primary school	Retain while the pupil remains at the primary school	Follow guidelines in 5.10 for pupils transferring to another school	Includes: • SEN reviews • Individual Education Plans (IEPs) / pupil profiles • Health questionnaires • Parental consent forms • Health care plans • Records of medicine administered
5.10	Pupil's educational record (pupil file) **All other pupils** • **Primary**	Yes	The Education (Pupil Information) (England) Regulations 2005	Retain while the pupil remains at the primary school, then: a) Pupil transfers to a known Local Authority primary or secondary school	**The file should follow the pupil when he/she leaves primary school:** a) Send pupil record to new school[3]	Includes: • Health questionnaires • Parental consent forms • Health care plans • Records of medicine administered

[3] In the case of exclusion it may be appropriate to transfer the record to the Education and Inclusion Service

				b) Pupil transfers to a known Local Authority or independent primary / secondary school which is another county within the UK; or transfers to an independent school	b) Send pupil record to new school, retaining a copy or summary until pupil is 22 years old, then destroy confidentially or delete securely		
				c) Pupil transfers to a known primary / secondary school outside of the UK	c) Send a copy of pupil record to new school, retaining original pupil record until pupil is 22 years old, then destroy confidentially or delete securely		

				d) Pupil transfers to an unknown school	d) Retain pupil file until pupil is 22 years old, then destroy confidentially or delete securely	
5.11	Pupil's educational record (pupil file) • Deceased pupils	Yes		Date of death + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.12	Images of pupils - signed consent forms by parent / guardian	Yes		Date of signing + 5 years; or at end of project; or when pupil leaves the school	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Images should not be reused outside of the time period or for other projects other than that specified on the form
5.13	Activity / visit / trip consent forms - signed by parent or guardian where no incident occurs	Yes		Date of event + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.14	Activity / visit / trip consent forms - signed by parent or guardian where a major incident occurs	Yes	Limitation Act 1980	Date of birth of child involved in incident + 22 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	**Important:** consent forms for ALL pupils for an event where a major incident occurs must be retained, not just that of the child involved
5.15	SATS results for individual pupils	Yes			Add to the main pupil file	

5.16	Internal examination papers (completed)	Yes		Current academic year + 6 years or until any appeals / validation process is complete	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.17	Internal and external examination results for individual pupils	Yes			Add to the main pupil file	
5.18	Examination results - summaries or other statistical information created by the school	Yes		Current academic year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
5.19	Any other records created in the course of contact with pupils maintained for teachers' own use (i.e. NOT part of the educational record)	Yes		Current academic year + 3 years	**Review** Review by school and EITHER allocate further retention period OR destroy as confidential waste or delete securely from electronic systems	

6.0	**Curriculum**					
6.1	Curricula records	No		Whilst operationally required	**Destroy** Destroy as confidential waste or delete securely from electronic systems	May include: • curriculum development records • lesson plans • syllabuses • schemes of work • timetables • mark books • records of homework set

7.0	**Human Resources**					
7.1	Interview notes and recruitment records (including pre-employment vetting information) • unsuccessful candidates	Yes		Date of interview + 1 year	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Includes: • proof of identity • proof of right to work in the UK
7.2	Interview notes and recruitment records (including pre-employment vetting information) • successful candidates	Yes		Follow retention period for 7.4	All recruitment information to be added to staff personnel file, except DBS checks (for DBS see 7.3)	

7.3	Pre-employment vetting information • successful candidates' DBS checks*	Yes	DfE 'Keeping Children Safe in Education' guidance (regularly updated)	Maximum of date of check + 6 months	**Destroy** Destroy as confidential waste or delete securely from electronic systems by the designated member of staff	*Formerly CRB checks Schools are not required to retain copies of DBS certificates. If the school chooses to do so, the copy must NOT be retained for longer than 6 months
7.4	Staff files (main personnel file)	Yes	Limitation Act (1980)	End of employment + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
7.5	Staff annual appraisal / assessment records	Yes		Current appraisal year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
7.6	Staff timesheets	Yes	Financial regulations	Current academic year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

7.7	Staff sickness records, excluding ill-health referrals (self-certification, doctor's certificates)	Yes		Current academic year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
7.8	Staff sickness records • ill health referrals	Yes	Limitation Act (1980)		Add to main personnel file and follow retention period for 7.4	
7.9	Staff maternity and paternity pay records	Yes	Statutory Maternity Pay Regulations (1986) (as amended)	Current academic year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
7.10	Disciplinary proceedings* • warnings	Yes			Add to main personnel file and follow retention period for 7.4	*for child protection / safeguarding disciplinary proceedings, see 7.13
7.11	Disciplinary proceedings* • substantiated or unsubstantiated	Yes		a) outcome letter: end of employ ment + 7 years b) all other records: close of case + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*for child protection / safeguarding disciplinary proceedings, see 7.13

7.12	Disciplinary proceedings* • false or malicious	Yes		a) outcome letter: end of employ ment + 7 years b) all other records: shred at close of case	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*for child protection / safeguarding disciplinary proceedings, see 7.13
7.13	Disciplinary proceedings* • safeguarding / child protection related	Yes	DfE 'Keeping Children Safe in Education' guidance (regularly updated)	Until normal pension age, or for 10 years from date of allegation, whichever is longer	**Destroy** Destroy as confidential waste or delete securely from electronic systems	*including where the allegation is unsubstantiated
7.14	Records of industrial tribunals, disciplinary panels, appeals	Yes	Limitation Act 1980 can apply		a) outcome letter: add to personnel file and follow retention period for 7.4 b) all other records: shred 7 years from end of process	
7.15	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		End of employment + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

8.0	**Health and Safety (H&S)**					
8.1	Health and safety policies	No		Life of policy + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.2	Risk assessments: general	No	Limitation Act (1980)	Date of risk assessment + 7 years (update regularly)	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.3	Risk assessments: exposure to noise, vibration, lead, asbestos, chemicals and biohazards (including COSHH)	No	Control of Substances Hazardous to Health Regulations (2002), Regulation 11 Control of Asbestos at Work Regulations (2012), Regulation 19	Date of risk assessment + 40 years (update regularly)	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.4	Risk assessments: exposure to radiation	No	Ionising Radiation Regulations 1999 (SI 1999/3232)	Date of risk assessment + 50 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

8.5	Accident reporting: adults a) accident books b) F2508-RIDDOR forms c) local accident investigation records	Yes	Social Security (Claims and Payments) Regulations (1979), Regulation 25 Social Security Administration Act (1992), Section 8. Limitation Act (1980)	(a) Current year + 3 (b) Current year + 3 (c) Current year + 3	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Accident reporting to be completed online and all copies to be held electronically
8.6	Accident reporting: children a) accident books b) F2508-RIDDOR forms c) local accident investigation records	Yes	Social Security (Claims and Payments) Regulations (1979), Regulation 25 Social Security Administration Act (1992), Section 8. Limitation Act (1980)	(a) Keep books until youngest child entered has reached age 22 (b) Date of birth of child + 22 years (c) Date of birth of child + 22 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Accident reporting to be completed online and all copies to be held electronically
8.7	Violent incident reporting (VIR)	Yes	Limitation Act (1980)	Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Accident reporting to be completed online and all copies to be held electronically
8.8	Physical intervention forms	Yes		Date of birth of child + 22 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

8.9	Fire precaution log books (e.g. records of drills and tests)	No	Limitation Act (1980)	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.10	Accessibility plans	Yes	Equalities Act (2010)	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.11	Health and safety training records	Yes		While current + 6 years, unless records apply for limited period (e.g. First Aid Certificates)	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.12	Maintenance records for any work equipment, including ladders, trollies, PPE, PAT etc.	No		Current year + 10 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
8.13	Health and safety inspection records, including: • site inspections • playground inspections	No		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

9.0	**Finance**					
9.1	Annual accounts	No		Retain in school for current year + 6 years	**Transfer to archive**	
9.2	Annual budget and background papers	No		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.3	Budget reports and budget monitoring records	No		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.4	Records covered by various financial regulations Including: invoices, receipts, order books, requisitions, delivery notices, petty cash records, records relating to the collection and banking of monies, records relating to the identification and collection of debt	No	Financial regulations	Current financial year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

9.5	Copy orders	No		Current year + 2 years, or current year + 6 years if included with delivery notes, invoices and receipts, etc.	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.6	Loans and grants managed by the school	No	Financial regulations	Date of last payment on loan + 12 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.7	School Fund records Including: cheque books, paying-in books, ledgers, invoices, receipts, bank statements, journey books	No	Financial regulations	Current financial year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.8	Contracts: under seal		Limitation Act (1980)	Contract completion date + 13 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.9	Contracts: under signature		Limitation Act (1980)	Contract completion date + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

9.10	Contracts: monitoring records			Current year + 2 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.11	Free school meals records	Yes	Financial regulations	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.12	School meals registers	Yes		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.13	School meals summary sheets	No		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	Formerly known as M1 forms
9.14	Applications for free school meals, travel, uniforms etc.	Yes	Financial regulations	Whilst child at school or current year + 6 years, whichever is the longest	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
9.15	Payroll records where school administers own payroll	Yes	Financial regulations	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

9.16	Records relating to individuals' pension details	Yes	Financial regulations	End of employment + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

10.0	**Property**					
10.1	Title deeds of all properties belonging to the school	No		Permanent	**Permanent** Retain in school whilst operational	
10.2	Plans of all properties belonging to the school	No		Permanent	**Permanent** Retain in school whilst operational	
10.3	Leases of properties leased by or to the schools	No		Expiry of lease + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.4	Records relating to the letting of school premises	No		Current year + 3 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.5	Burglary, theft and vandalism report forms			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.6	All records relating to the maintenance of the school, including maintenance log books	No		Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

10.7	Inventories of equipment and furniture			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
10.8	Insurance papers			While current	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

11.0	**Adult and Community Learning and Activities**					
11.1	Annual funding agreements			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
11.2	Enrolment forms, fee receipts, refund records, course registers, banking records			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
11.3	LSC capital grants, expenditure records			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
11.4	Community management agreements			Life of agreement + 7 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
11.5	Minutes of governors' management committees			Permanent	**Permanent** Retain in school for 6 years	

11.6	Income records for centre-run activities			Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
11.7	Notice of successful applications for external funding, and conditions attached to grants			Period of funding or length of funding agreement (e.g. capital schemes) + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	
11.8	Adult learning course programmes and brochures			Current year + 3 years	**Transfer to archive**	
11.9	Records relating to the letting of school facilities to community or other groups, including after-school and holiday clubs	Yes	Statute of Limitations 1980	Current year + 6 years	**Destroy** Destroy as confidential waste or delete securely from electronic systems	

Appendix 8

St Mary's Catholic Primary School

Subject Access Request Form

Name of data subject:	
Date of request:	**Date of deadline (+ 1 month of receiving all necessary information and fee if required):**
Information requested:	

Question	Yes / No	Next action	Completed date and initials
Was the request made in writing?		If no contact immediately to request a written enquiry	
Would you usually provide this information in the normal course of business?		If yes, provide this information promptly.	
Do you need further information or clarification?		If yes, contact the requester as soon as possible.	
Has the identity of the requester been proven?		If not, ask for any evidence you need to confirm it.	
Is a fee required?		Request fee immediately.	Received
Do we hold the information requested?		If no inform the requester.	
Will the information change within the timeframe?		If yes, remember only routine amendments may be made.	
Does the information include details about other people?		Third party details must not be given without consent. Give as much information by editing any reference to third parties. www.ico.gov.uk for detailed guidance	
Is the information exempt?		If exempt reply saying we do not hold any	

		information which we are required to disclose. www.ico.gov.uk for more information.	
Are there complex terms or codes?		**Explain all terms/codes/jargon in simple language.**	
Has a copy of the information been supplied in a permanent form?		**If this is impossible and the individual agrees they may be able to view the information on screen.**	
Has the subject access request been completed according to ICO guidelines and within the timeframe.		**If not details should be given as to why this was not completed and reported to the Headteacher**	

Appendix 9

Subject Access Request Guidance

See link below

https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf

Appendix 10

Data Privacy Impact Assessments (DPIA)

Guide to completing a DPIA

A DPIA is a process which helps an organisation to identify and reduce the privacy risks to individuals whose personal information is used in a project. The General Data Protection Regulation (GDPR) will make it a legal requirement to carry out a DPIA where the use of the personal information is likely to result in a **high** risk to the privacy of individuals

Examples might include use of new technologies, including proposals to use cloud storage facilities for school information, use of software that uses details from the SIMS database, use of CCTV and biometrics, such as finger print scanning.

A DPIA can be used to help you to design more efficient and effective ways for handling personal data, minimise privacy risks to the individuals affected and financial and reputational impact of a data incident on the school.

This guide is intended to help you assess whether a DPIA is needed, identify levels of risk of personal data for your project and complete a DPIA report (where applicable), which will need to be agreed and approved by (complete as appropriate – Data Protection Officer/Head Teacher).

When to carry out a DPIA

A PIA should be completed when the project is likely to involve collection of personal data that may involve a high risk to the privacy of individuals. You should take into account the following when deciding whether a DPIA is necessary

1. If personal data is not being collected or processed there is no need to do a DPIA.
2. Will the project involve the collection of new or different types of information about individuals? If personal information will be collected using new technology, or collection of a new type of special category data not collected before, you should carry out a DPIA. If you will be collecting large amounts of personal information to use in a way not previously used, you should complete a DPIA
4. Any project involving monitoring of individuals, such as installation of new CCTV, should always require a DPIA as should any use of biometric technology

When to start a DPIA

If you are thinking about starting a project or making changes to existing services/ systems, then you should consider whether a DPIA is necessary from an early stage.

A DPIA should be started at project initiation stage, continued throughout the life of the project and re-visited in each new project phase, for example, when you want to use the personal data for a new or additional purpose for the use of the data, or if you are collecting new personal data. This should be proportionate to the level of special category data being collected or processed as a result of the project.

It is important to start at an early stage of the process to allow for time to resolve issues and mitigate for any risks identified, in order to avoid the difficulties of having to address these points late in the project when other decisions have already been made.

How to carry out a DPIA

Use the checklist below to help you decide whether the project involves privacy risks, identify what they are and work out what steps you will need to take to minimise those risks as far as possible.

When you have considered all of the risks, you should come to a conclusion about anything you can do to eliminate or minimise the risks you have identified. Some examples might include:-

- Minimising the risks of collecting too much personal information on CCTV by siting and angling the cameras so that they are focussed only on perhaps the car park rather than the entire school playground, or the entrance door, not into the school office

- Checking the questions you have asked on a form before you send it out and ensuring that you really need all of the personal information you have requested
- If you need to store personal information on paper records ensuring that you keep them in a secure location which cannot be readily accessed by unauthorised individuals.
- If using a laptop in a classroom, make sure that staff are instructed to lock the screen if they leave it unattended for a while

When you have recorded all of these points and how you will address the risks, you should get it signed off – either by the Data Protection Officer (or if the Data Protection Officer is completing the form, perhaps by the Headteacher) and keep a copy to refer back to for audit purposes and for updating if the project is changed or extended in future.

Completing a DPIA

When you have completed the DPIA, considered any risks and mitigated them wherever possible, the school will need to decide whether to accept any remaining risks. It is good practice to document what risks were identified, what steps were taken to minimise them and what risks were accepted.

You will also need to consider who should sign off the final DPIA – e.g. Headteacher, Data Protection Officer.

You can find more detailed guidance on conducting privacy impact assessments on the ICO's DPIA code of practice (currently in draft form)

https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

Checklist

Project name

Brief description of project.

1. What is the project for? What does it seek to achieve?
2. Will the project collect information about individuals e.g. students, parents, staff? If no personal information is collected, a DPIA will not be required.
3. What type of information will it collect? Will it be special category data? e.g.

information about an individuals physical or mental health, social care details, details of criminal offences or allegations, or collecting large quantities of personal information? Any of these will raise the level of risk.
4. How will the information be collected? On paper forms? Electronically? Who will have access to this information? How will it be stored and kept secure?
5. How will pupils/staff /parents be made aware of how their personal information is being used? Will a privacy notice be provided? At the end of a paper form? By linking to the school website privacy notice? Does the privacy notice provide sufficient detail about the reasons for collecting the information and who it may be shared with?
6. Do you need consent from the individual to use the information? e.g. because special category data is being collected.

7. Does the project involve the use of new or different technology which could be privacy intrusive e.g. CCTV, monitoring of staff, biometrics, GPS tracking or cloud storage
8. What risks have been identified? What steps have been taken to eliminate or minimise them?
Signature Name (printed) Position Date

Appendix 11

DATA BREACH REPORTING FORM

The aim of this document is to ensure that, in the event of a security incident such as personal data loss, information can be gathered quickly to document the incident, its impact and actions to be taken to reduce any risk of harm to the individuals affected.

The checklist can be completed by anyone with knowledge of the incident. It will need to be submitted and reviewed by the Data Protection Officer who can determine the implications for the school, assess whether changes are required to existing processes and notify the ICO / data subject where appropriate.

SUMMARY OF INCIDENT	
Data and time of incident	
Nature of breach (e.g. theft/ disclosed in error/ technical problems)	
Give a full description of how breach occurred	
PERSONAL DATA	
Give a full description of all the types of personal data involved with the breach but not specifically identifying the individual concerned (e.g. name, addresses, health information etc.)	
How many individuals are affected?	
Have the affected individuals been informed of the incident?	
Is there any evidence that the personal data involved in this incident has been further	

disclosed? If so, please provide details	
IMPACT OF INCIDENT	
What harm is foreseen to the individuals affected? (e.g. could the breach increase the risk of identity theft?)	
What measures have been taken to minimise the impact of the incident?	
Has the data been retrieved or deleted? If yes, state when and how	
REPORTING	
Who became aware of the breach?	
How did they become aware of the breach?	
Form Completed by	
Position	
Date	