Jubilee
PRIMARY SCHOOL

Data Protection Policy

May 2022

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 UK data protection law.

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

2. Legislation and guidance

This policy meets the requirements of the

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

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

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 • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

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 Board of Trustees

The Board of Trustees 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.

Where relevant, the DPO will report to the board their advice and recommendations on school data protection issues. The DPO is also the first point of contact for the ICO.

We outsource or DPO responsibilities to 'Cantium Business Solutions: DPO Services'.

Address: DPO Services, iSYSTEMS Integration, Devonshire House, 29-31 Elmfield Road,Bromley, Kent BR1 1LT.

Our DPL (Data Protection Lead) is Laura Payne and is contactable via:
e-mail: assistantheadLP@jubileeprimaryschool.org.uk
Tel: 01622 808873

It is the DPL's responsibility to provide and annual report of activities directly to the Board of Trustees. The DPL is also the first point of contact for individuals whose data the school processes.

5.3 Headteacher

The Headteacher 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 DPL 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 UK.
- If there has been a data breach.
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
- If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

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

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 under data protection law:

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

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

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

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

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

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).

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Staff should adhere to the KCC Information Management Toolkit for Schools on KELSI with reference to the Record Retention Schedule, available at the following link: http://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information/records-management (See **Appendix 2** for information)

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 UK data protection law.
    - Establish a contract with the supplier or contractor 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 internationally, we will do so in accordance with UK 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The safeguards provided if the data is being transferred internationally

Subject access requests must be submitted in writing, either by letter or email. 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 (or receipt of the additional information needed to confirm identity, where relevant).
- 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 may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child has been or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover 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.
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 DPL. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

There is no automatic parental right of access to the educational record of a child, however, at Jubilee Primary School we can provide this. Parents can submit a written request to the Headteacher to gain access to their child's educational record (which includes most information about a pupil) within 30 school days of receipt of the written request. If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it. There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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 Laura Payne DPL.

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

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 data protection 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply.
- 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, any transfers outside of the UK and the safeguards for those, 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 password protected and 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, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff are expected to follow the same procedures as within school, for example confidential information must not be left anywhere where there is general access.
- 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 or reuse passwords form other sites.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff 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 acceptable use agreement).
- 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).
- Where personal information is contained within documents, names will not appear e.g. a document will read 'Diagnosed with...'..
- When using electronic devices to compose documents, the practice of using an existing template, or cutting and pasting from a previous document, is strictly prohibited. A blank template will be used every time to prevent the corruption of a report.
- All letters will be hand delivered to parents.
- Staff are encouraged to double check emails, use the 'BCC' option and activate email delaying.

15. Disposal of records

Personal data that is no longer needed will be disposed of securely at least once every term, based on the retention period. 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 after becoming aware of it. 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 annually and shared with the full Board of Trustees.

19. Links with other policies

- Freedom of Information Policy

- Child Protection and Safeguarding Policy

- Acceptable Use Policy

Governor Approval and Review Dates

This document was approved by the full Board of Trustees in May 2022. It will be reviewed in May 2023.

Changes since the last version

Version	Date	Amendment
V2	May 2022	Appendix 2: Updated KCC Information
V2	May 2022	Appendix 1: Wording updated for more clarity.
V2	May 2022	Section 14: Updates and further preventative measures
V2	May 2022	Section 13: Updated wording for clarity to reflect new UK data protection law.
V2	May 2022	Section 12: Reference to parents personal use of videos and photographs.
V2	May 2022	Section 11: Guidance updated.
V2	May 2022	Section 10: Wording updated for clarity.
V2	May 2022	Section 9.4: Wording updated for clarity.
V2	May 2022	Section 9.3: The DPA and latest ICO guidance.
V2	May 2022	Section 9.1: Bullet points added to ensure clarity.
V2	May 2022	Section 8: Changes to reflect new UK data protection law.
V2	May 2022	Section 7.2: Sentence added for clarity.
V2	May 2022	Section 7.1: Deleted the paragraph about gaining consent when offering online services to pupils.

V2	May 2022	Section 7.1: Further detail added to reflect the DPA 2018.
V2	May 2022	Section 6: Replaced 'GDPR' with 'UK GDPR'.
V2	May 2022	Section 5.4: Transferring personal data from outside the EEA (European Economic Area)
V2	May 2022	Section 5.2: DPO / DPL information updated.
V2	May 2022	Section 2: Added lick to the UK GDPR
V2	May 2022	Section 1: Removed links to EU legislation and replaced with a reference to 'UK data protection law'.
V1	May 2020	Appendix 1 added GDPRis software

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 DPL who will notify the DPO.
- The DPO, alongside the DPL, 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 DPL will alert the Headteacher and the Chair of Trustees
- The DPO, with the DPL, 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, before and after the implementation of steps to mitigate the consequences.
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool. 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 within the GDPRIs system.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours of the schools awareness of the breach. 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 of the school's awareness of the breach. 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
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - 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 consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individual – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach on the GDPRis software, 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)
- 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 the designated GDPRis software.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

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
- 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.
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its safeguarding partners.

Other types of breach

- 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.

Appendix 2: KCC Recommended Retention Periods

Information Management Toolkit for Schools Version 2 (August 2018)

Where the Protective Marking column is blank, the record series should be considered to be "NOT PROTECTIVELY MARKED"

IMTKS1 Governing Body

For further information about governing body records please see: "The constitution of governing bodies of maintained schools Statutory guidance for governing bodies of maintained schools and local authorities in England August 2017"

				Information Asset Register Information						Information Risk Register Information
	Basic file description	**Statutory Provisions**	**Retention Period**	**Information Asset Owner**	**Principal Copy**	**Principal Record Keeper**	**Business Critical**	**Personal Information**	**Protective Marking**	**Information Risk Category**
IMTKS1A	**Management of Governing Body**									
IMTKS1A.1	Instruments of Government		Permanent				YES	No		
IMTKS1A.2	Trusts and Endowments		Permanent				YES	No		
IMTKS1A.3	Records relating to the election of parent and staff governors not appointed by the governors		Date of election + 6 months				YES	Yes	OFFICIAL	
IMTKS1A.4	Records relating to the appointment of co-opted governors		Provided that the decision has been recorded in the minutes the records relating to the appointment can be destroyed once the co-opted governor has finished their term of office				YES	Yes	OFFICIAL	
IMTKS1A.5	Records relating to the election of chair and vice chair		Once the decision has been recorded in the minutes, the records relating to the election can be destroyed				YES	Yes	OFFICIAL	
IMTKS1A.6	Scheme of Delegation and Terms of Reference for Committees		PERMANENT				YES	No		
IMTKS1A.7	Meetings Schedule		Current year				YES	No		
IMTKS1A.8	Agendas – Principal copy	The School Governance (Roles, Procedures and Allowances) (England) Regulations 2013	Permanent				YES	No		
IMTKS1A.9	Minutes - Principal set (signed)	As above	Permanent				YES	Yes	OFFICIAL	
IMTKS1A.10	Reports made to the Governors' Meeting which are referred to in the minutes	As above	Permanent				YES	Yes	OFFICIAL	
IMTKS1A.11	Register of attendance at Full Governing Board meetings	As above	Date of last meeting in the book + 6 years				YES	Yes	OFFICIAL	
IMTKS1A.12	Papers relating to the management of the Annual Parents' Meeting	The Education (Annual Parents' Meetings) (England) Regulations 1999[1]	Date of meeting + 6 years				YES	Yes		
IMTKS1A.13	Agendas – Additional Copies		Date of meeting				NO	No		
IMTKS1A.14	Minutes - Inspection copies		Date of meeting + 3 years				NO	Yes		

[1] Statutory Instruments 1999 No 2014

				Information Asset Register Information						Information Risk Register Information
	Basic file description	**Statutory Provisions**	**Retention Period**	**Information Asset Owner**	**Principal Copy**	**Principal Record Keeper**	**Business Critical**	**Personal Information**	**Protective Marking**	**Information Risk Category**
IMTKS1A.15	Records relating to Governor Monitoring Visits		Date of the visit + 3 years				YES	Yes	OFFICIAL	
IMTKS1A.16	Annual Reports required by the Department for Education	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI	Date of report + 10 years				YES	No		
IMTKS1A.17	All records relating to the conversion of schools to Academy status		PERMANENT				YES	No		
IMTKS1A.18	Records relating to complaints made to and investigated by the Governing Body		Date of resolution of complaint + 6 years then review for further retention in the case of contentious disputes				YES	Yes	OFFICIAL SENSITIVE	
IMTKS1A.19	Correspondence sent and received by the Governing Body		Current year + 6 years				YES	Yes	OFFICIAL	
IMTKS1B	**Management of Governors**									
IMTKS1B.1	Records relating to the appointment of a clerk to the Governing Body		Date appointment as clerk ceases + 6 years				YES	Yes	OFFICIAL	
IMTKS1B.2	Records relating to the terms of office of serving governors including evidence of appointment		PERMANENT				YES	Yes	OFFICIAL	
IMTKS1B.3	Records relating to Governor Declaration against disqualification criteria		Until the Governor steps down				YES	Yes	OFFICIAL	
IMTKS1B.4	Register of Business Interests		PERMANENT				YES	Yes		
IMTKS1B.5	Governors Code of Conduct		This is expected to be a dynamic document, one copy of each version should be kept permanently				YES	Yes		
IMTKS1B.6	Records relating to the training required and received by Governors		Until the Governor steps down				YES	Yes	OFFICIAL	
IMTKS1B.7	Records relating to the induction programme for new governors		Until the Governor steps down				YES	Yes	OFFICIAL	
IMTKS1B.8	Records relating to DBS checks carried out on clerk and members of the governing body		Date of DBS check + 6 months				YES	Yes	OFFICIAL	

IMTKS2 Pupil Management

				Information Asset Register Information						Information Risk Register Information
	Basic file description	**Statutory Provisions**	**Retention Period**	**Information Asset Owner**	**Principal Copy**	**Principal Record Keeper**	**Business Critical**	**Personal Information**	**Protective Marking**	**Information Risk Category**
IMTKS2A	**Admissions and Attendance**									
IMTKS2A.1	Admission Registers		Permanent				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS2A.2	Records relating to the admissions process – if the admission is successful		Admission + 1 year				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS2A.3	Admissions – if the appeal is unsuccessful		Resolution of case + 1 year				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS2A.4	Admissions – Secondary Schools – Casual		Current year + 1 year				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS2A.5	Proofs of address supplied by parents as part of the admissions process		Current year + 1 year				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS2A.6	Attendance registers		Date of register + 3 years				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS2A.7	Letters authorising absence		Date of absence + 2 years				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS2B	**Pupil Educational Record**									
IMTKS2B.1	Pupil Files and/or record cards - Primary	Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437)	Retain for the time which the pupil remains at the Primary School Transfer to the Secondary School (or other Primary School) when the child leaves the school[2]				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS2B.2	Pupil Files and/or record cards - Secondary	Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437)	DOB of the pupil + 25 years[1]				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS2B.3	Examination results - Public		Year of examinations + 6 years[3]				No	Yes		
IMTKS2B.4	Examination results - Internal examination results		Current year + 5 years If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary				No	Yes		
IMTKS2B.5	Any other records created in the course of contact with pupils		Current year + 3 years then review				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS2B.6	Images held of pupils together with any consents and permissions to publish		All records relating to the image should be retained for the life of the image. The length of time the image is to be retained should be included on the privacy statement				Yes	Yes	OFFICIAL	
IMTKS2C	**Special Educational Needs**									
IMTKS2C.1	Special Educational Needs files, reviews and Individual Education Plans		DOB of the pupil + 25 years				Yes	Yes	OFFICIAL SENSITIVE	

[2] In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service. If the pupil has left the primary school and there is no information about which school that the pupil has moved onto, or they have moved onto elective home education, or the pupil has moved abroad or to an independent school, then the records can be sent to Elizabeth Barber, Room 2.89 Sessions House, Maidstone for archiving.
[3] Any certificates left unclaimed should be returned to the appropriate Examination Board

				Information Asset Register Information						Information Risk Register Information
	Basic file description	Statutory Provisions	Retention Period	Information Asset Owner	Principal Copy	Principal Record Keeper	Business Critical	Personal Information	Protective Marking	Information Risk Category
IMTKS2C.2	Statement maintained under The Education Act 1996 - Section 324	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years Unless legal action is pending				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS2C.3	Proposed statement or amended statement	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years Unless legal action is pending				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS2C.4	Advice and information to parents regarding educational needs	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years Unless legal action is pending				No	Yes	OFFICIAL SENSITIVE	
IMTKS2C.5	Accessibility Strategy	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years Unless legal action is pending				Yes	No	OFFICIAL SENSITIVE	
IMTKS2C.6	Pupil SEN Files		DOB of pupil + 25 years then review unless legal action is pending. If so, it may be appropriate to add an additional retention period.				Yes	Yes	OFFICIAL SENSITIVE	

IMTKS3 School Trips and Extra Curricular Activities

				Information Asset Register Information						Information Risk Register Information
	Basic file description	Statutory Provisions	Retention Period	Information Asset Owner	Principal Copy	Principal Record Keeper	Business Critical	Personal Information	Protective Marking	Information Risk Category
IMTKS3A	**Educational Visits outside the Classroom**									
IMTKS3A.1	Primary Schools Records created by schools to obtain approval to run an Educational Visit outside the Classroom[4]	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998)	Date of visit + 14 years[5]				Yes	No	OFFICIAL SENSITIVE	
IMTKS3A.2	Secondary Schools Records created by schools to obtain approval to run an Educational Visit outside the Classroom[3]	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998)	Date of visit + 10 years[4]				Yes	No	OFFICIAL SENSITIVE	
IMTKS3B	**Day Trips**									
IMTKS3B.1	Parental permission slips for school trips – where there has been no major incident		Conclusion of the trip				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS3B.2	Parental permission slips for school trips – where there has been a major incident	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS3C	**Residential Trips**									
IMTKS3C.1	All records relating to the organization of school residential trips	Limitation Act 1980	Date of the residential visit + a minimum of 6 years then review				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS3D	**Walking Bus**									

[4] including GOF1 and GOF2 and data entered on the e-go system
[5] This retention period has been set in agreement with the Safeguarding Children's Officer

				Information Asset Register Information						Information Risk Register Information
	Basic file description	Statutory Provisions	Retention Period	Information Asset Owner	Principal Copy	Principal Record Keeper	Business Critical	Personal Information	Protective Marking	Information Risk Category
IMTKS3D.1	Walking Bus registers		Date of register + 3 years[6]				Yes	Yes	OFFICIAL SENSITIVE	

IMTKS4 School Management – Teaching and Curriculum

				Information Asset Register Information						Information Risk Register Information
	Basic file description	Statutory Provisions	Retention Period	Information Asset Owner	Principal Copy	Principal Record Keeper	Business Critical	Personal Information	Protective Marking	Information Risk Category
IMTKS4A	**Senior Management Team**									
IMTKS4A.1	Log Books		Date of last entry in the book + 6 years				Yes	No		
IMTKS4A.2	Minutes of the Senior Management Team and other internal administrative bodies		Date of meeting + 5 years				Yes	Yes	OFFICIAL	
IMTKS4A.3	Reports made by the Head Teacher or the management team		Date of report + 3 years				Yes	Yes	OFFICIAL	
IMTKS4A.4	Records created by Head Teachers, Deputy Head Teachers, Heads of Year and other members of staff with administrative responsibilities		Closure of file + 6 years				Yes	Yes	OFFICIAL	
IMTKS4A.5	Correspondence created by Head Teachers, Deputy Head Teachers, Heads of Year and other members of staff with administrative responsibilities		Date of correspondence + 3 years				Yes	Yes	OFFICIAL	
IMTKS4A.6	School development plans		Closure + 6 years then review				Yes	No		
IMTKS4A.7	Professional development plans		Closure + 6 years				Yes	Yes	OFFICIAL	
IMTKS4A.8	Action Plans		Date of action plan + 3 years				Yes	No		
IMTKS4A.9	Policy documents		Expiry of policy Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)				Yes	No		
IMTKS4B	**Curriculum Management**									
IMTKS4B.1	Timetable		Current year then review				No	No		
IMTKS4B.2	Curriculum development		Current year + 6 years				No	No		
IMTKS4B.3	Curriculum returns		Current year + 3 years				No	No		
IMTKS4B.4	School syllabus		Current year then review				No	No		
IMTKS4B.5	Schemes of work		Current year then review				No	No		
IMTKS4B.6	Class record books		Current year then review				No	No		
IMTKS4B.7	Mark Books		Current year then review				No	No		
IMTKS4B.8	Record of homework set		Current year then review				No	No		
IMTKS4B.9	Pupils' work		Current year then review				No	No		
IMTKS4B.10	SATS records including examination results. Exam papers should only be retained if they are required to evidence the results		Current year + 6 years				Yes	Yes	OFFICIAL SENSITIVE	

[6] This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting

IMTKS5 Management of Schools - Administration

				Information Asset Register Information						Information Risk Register Information
	Basic file description	**Statutory Provisions**	**Retention Period**	**Information Asset Owner**	**Principal Copy**	**Principal Record Keeper**	**Business Critical**	**Personal Information**	**Protective Marking**	**Information Risk Category**
IMTKS5A	**Personnel Management**									
IMTKS5A.1	Employer's Liability certificate		Closure of the school + 40 years				Yes			
IMTKS5A.2	Staff Personal files		Termination + 6 years[7]				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5A.3	Interview notes and recruitment records		Date of interview + 6 months				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5A.4	Pre-employment vetting information (including DBS checks)[8]	DBS guidelines	Date of check + 6 months				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5A.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file.				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5A.6	Right to Work in the UK checks	https://www.gov.uk/check-job-applicant-right-to-work	Termination of employment + 2 years				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5A.7	Disciplinary proceedings: case not found		Take advice from Personnel if the proceedings were child protection related otherwise destroy immediately at the conclusion of the case				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5A.8	Disciplinary proceedings: written warnings		The duration of the warning [9]				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5A.9	Annual appraisal or assessment records		Current year + 5 years				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5A.10	Images held of members of staff together with any consents and permissions to publish		All records relating to the image should be retained for the life of the image. The length of time the image is to be retained should be included on the privacy statement				Yes	Yes	OFFICIAL	
IMTKS5B	**Health and Safety**									
IMTKS5B.1	Policy Statements		Date of expiry + 1 year [it may be necessary to keep one copy of each policy so that a history of what policies were in place at any time]				Yes	No		
IMTKS5B.2	Accessibility Plans	Disability Discrimination Act 1995	Current year + 6 years				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5B.3	Records relating to accident/injury at work	The Management of Health & Safety at Work Regulations 1999 Health and Safety at Work Act 1974	Date of incident + 12 years [10]				Yes	Yes	OFFICIAL SENSITIVE	

[7] These files should be subject to KCC's open file policy where the employees are employed by Kent County Council as the Local Authority
[8] Please note that schools must not keep copies of the documents which are checked for DBS purposes.
[9] If this information has been added to an individual's personnel file, it must be weeded from the file once the retention period has elapsed
[10] In the case of serious accidents a further retention period will need to be applied

				Information Asset Register Information						Information Risk Register Information
	Basic file description	**Statutory Provisions**	**Retention Period**	**Information Asset Owner**	**Principal Copy**	**Principal Record Keeper**	**Business Critical**	**Personal Information**	**Protective Marking**	**Information Risk Category**
IMTKS5B.4	Accident Reporting – Children	Limitation Act 1980	Date of birth + 22 years where the injured person is a minor at the time of the accident				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5B.5	Accident Reporting – Adults	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	Date of the accident + 4 years where the injured person is an adult at the time of the accident;				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5B.6	Risk Assessments	The Management of Health & Safety at Work Regulations 1999 Health and Safety at Work Act 1974	Current year + 3 years				Yes	No		
IMTKS5B.7	COSHH Risk Assessments	Control of Substances Hazardous to Health (COSHH) Regulations 2002	Date of creation + 40 years				Yes	No		
IMTKS5B.8	Incident reports		Current year + 20 years				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5B.9	Process of monitoring areas where employees and persons are likely to have become in contact with asbestos	Control of Asbestos Regulations 2012	Last action + 40 years				Yes	No		
IMTKS5B.10	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation	Ionising Radiations Regulations 2017	Last action + 50 years				Yes	No		
IMTKS5B.11	Fire Safety Records including Fire Safety Audits	Regulatory Reform (Fire Safety) Order 2005	Current year + 6 years				Yes	No		
IMTKS5B.12	Fire Risk Assessments	Regulatory Reform (Fire Safety) Order 2005	Date the fire risk assessment expires + 6 years							
IMTKS5B.13	Fire Drill records	Regulatory Reform (Fire Safety) Order 2005	Date of fire drill + 6 years				Yes	No		
IMTKS5C	**Payroll and Pensions**									
IMTKS5C.1	Records relating to the management of the payroll	HMRC - Compliance Handbook Manual CH15400	Financial year to which the payroll is run + 6 years							
IMTKS5C.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Retirement Benefits Schemes (Information Powers) Regulations 1995	Current year + 6 years				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5C.3	Salary cards		Last date of employment + 85 years				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5C.4	Maternity pay records	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year + 3yrs				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5C.5	Timesheets, sick pay	HMRC - Compliance Handbook Manual CH15400	Current year + 6 years				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5D	**Financial Records**									
IMTKS5D.1	Annual Accounts	HMRC - Compliance Handbook Manual CH15400	Current year + 6 years				Yes	No		
IMTKS5D.2	Loans and grants	HMRC - Compliance Handbook Manual CH15400	Date of last payment on loan + 12 years then review to see whether a further retention period is required				Yes	No	NOT PROTECTIVELY MARKED	

				Information Asset Register Information						Information Risk Register Information
	Basic file description	**Statutory Provisions**	**Retention Period**	**Information Asset Owner**	**Principal Copy**	**Principal Record Keeper**	**Business Critical**	**Personal Information**	**Protective Marking**	**Information Risk Category**
IMTKS5D.3	Inventories of equipment and furniture		Current year + 6 years				No	No		
IMTKS5D.4	Annual Budget and background papers		Current year + 6 years				Yes	No		
IMTKS5D.5	Budget reports, budget monitoring etc		Current year + 3 years				Yes	No		
IMTKS5D.6	Contracts - under seal	Limitation Act 1980 (Section 12)	Contract completion date + 12 years				Yes	No		
IMTKS5D.7	Contracts - under signature	Limitation Act 1980 (Section 2)	Contract completion date + 6 years				Yes	No		
IMTKS5D.8	Contracts - monitoring records		Current year + 2 years				Yes	No		
IMTKS5D.9	Order books and requisitions		Current year + 6 years				Yes	No		
IMTKS5D.10	Copy orders		Current year + 2 years				No	No		
IMTKS5D.11	Delivery Documentation		Current year + 6 years				Yes	No		
IMTKS5D.12	Invoice, receipts and other records covered by the HMRC - Compliance Handbook Manual CH15400	HMRC - Compliance Handbook Manual CH15400	Current year + 6 years				Yes	No		
IMTKS5D.13	Petty cash books	HMRC - Compliance Handbook Manual CH15400	Current financial year + 6 years				Yes	No		
IMTKS5D.14	Debtors' Records	HMRC - Compliance Handbook Manual CH15400	Current year + 6 years				Yes	Yes		
IMTKS5D.15	Applications for free school meals, travel, uniforms etc		Whilst child is at school				No	Yes	OFFICIAL	
IMTKS5D.16	Student grant applications		Current year + 3 years				Yes	Yes	OFFICIAL	
IMTKS5D.17	School Fund Records[11]	HMRC - Compliance Handbook Manual CH15400	Current year + 6 years				Yes	No		
IMTKS5E	**Building Management**									
IMTKS5E.1	Title Deeds		Permanent [12]				Yes	No		
IMTKS5E.2	Plans		Permanent Retain in school whilst operational				Yes	No	OFFICIAL [13]	
IMTKS5E.3	Records relating to maintenance and contractors	HMRC - Compliance Handbook Manual CH15400	Current year + 6 years				Yes	No		
IMTKS5E.4	Maintenance log books		Last entry + 10 years				Yes	No		
IMTKS5E.5	Contractors' Reports		Current year + 6 years				Yes	No		
IMTKS5E.6	Leases		Expiry of lease + 6 years				Yes	No		
IMTKS5E.7	Lettings		Current year + 3 years				Yes	No		
IMTKS5E.8	Burglary, theft and vandalism report forms		Current year + 6 years				Yes	No		
IMTKS5E.9	Records relating to legionella and water checks	The Management of Health & Safety at Work Regulations 1999 Health and Safety at Work Act 1974	Date of check + 3 years				Yes	No		
IMTKS5F	**School Meals**									
IMTKS5F.1	Dinner Register		Current year + 3 years				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS5F.2	School Meals Summary Sheets		Current year + 3 years				No	No		
IMTKS5F.3	Free school meals registers	HMRC - Compliance Handbook Manual CH15400	Current year + 6 years				Yes	Yes	OFFICIAL	
IMTKS5G	**General Administration**									

[11] including cheque books, paying in books, ledgers, invoices, receipts, bank statements, school journey books
[12] these should follow the property unless the property has been registered at the Land Registry
[13] These records carry an OFFICIAL marking as there can be security issues about allowing access to the plans of buildings to people who may be looking to burgle the premises

				Information Asset Register Information						Information Risk Register Information
	Basic file description	Statutory Provisions	Retention Period	Information Asset Owner	Principal Copy	Principal Record Keeper	Business Critical	Personal Information	Protective Marking	Information Risk Category
IMTKS5G.1	School brochure/prospectus		Current year + 3 years				No	No		
IMTKS5G.2	General file series or correspondence files		Current year + 5 years				No	No		
IMTKS5G.3	Circulars (staff/parents/pupils)		Current year + 1 year				No	No		
IMTKS5G.4	Newsletters, ephemera		Current year + 1 year				No	No		
IMTKS5G.5	Visitors book		Current year + 2 years				No	Yes	OFFICIAL	
IMTKS5G.6	Images held of pupils together with any consents and permissions to publish		All records relating to the image should be retained for the life of the image. The length of time the image is to be retained should be included on the privacy statement				Yes	Yes	OFFICIAL	
IMTKS5G.7	Records relating to the management of PTA/Old Pupils Associations		Current year + 6 years				No	Yes	OFFICIAL	
IMTKS5G.8	Records relating to the management of data subject access requests		Current year + 3 years				No	Yes	OFFICIAL	
IMTKS5G.9	Records relating to the management of freedom of information requests		Current year + 3 years				No	Yes	OFFICIAL	

IMTKS6 Management of Schools – Safeguarding

				Information Asset Register Information						Information Risk Register Information
	Basic file description	Statutory Provisions	Retention Period	Information Asset Owner	Principal Copy	Principal Record Keeper	Business Critical	Personal Information	Protective Marking	Information Risk Category
IMTKS6A	**Adults**									
IMTKS6A.1	Records of allegations about workers who have been investigated and found to be without substance	Information Commissioner Code of Practice: Employment Records 2002 - "Child Protection Procedures for Managing Allegations Against Staff within Schools and Education Services" (September 2008) p17	These records should not normally be retained once an investigation has been completed[14].				Yes	Yes	OFFICIAL SENSITIVE	
IMTKS6A.2	Outcome of an allegation made against a staff member	Safeguarding Children in Education Guidelines: Dealing with Allegations of Abuse against Teachers and Other Staff Safeguarding Children in Education and Safer Recruitment 2007 Para 5.1	Until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer				Yes	Yes	OFFICIAL SENSITIVE	

IMTKS7 Central Government and Local Authority

[14] There are some exceptions to this where for its own protection the employer has to keep a limited record that an allegation was received and investigated, for example where the allegation relates to abuse and the worker is employed to work with children or other vulnerable adults

				Information Asset Register Information						Information Risk Register Information
	Basic file description	**Statutory Provisions**	**Retention Period**	**Information Asset Owner**	**Principal Copy**	**Principal Record Keeper**	**Business Critical**	**Personal Information**	**Protective Marking**	**Information Risk Category**
IMTKS7A	**Local Authority**									
IMTKS7A.1	Secondary transfer sheets (Primary)		Current year + 2 years				No	Yes	OFFICIAL SENSITIVE	
IMTKS7A.2	Attendance returns		Current year + 1 year				No	No		
IMTKS7A.3	Circulars from LA		Whilst required operationally then review to see whether a further retention period is required				No	No		
IMTKS7B	**Central Government**									
IMTKS7B.1	OFSTED reports and papers		Replace former report with any new inspection report then review to see whether a further retention period is required				No	No		
IMTKS7B.2	Returns		Current year + 6 years				No	No		
IMTKS7B.3	Circulars from DfE		Whilst operationally required then review to see whether a further retention period is required				No	No		

IMTKS8 Family Liaison Officers and Parent Support Assistants

				Information Asset Register Information						Information Risk Register Information
	Basic file description	**Statutory Provisions**	**Retention Period**	**Information Asset Owner**	**Principal Copy**	**Principal Record Keeper**	**Business Critical**	**Personal Information**	**Protective Marking**	**Information Risk Category**
IMTKS8.1	Day Books		Current year + 2 years then review				No	Yes	OFFICIAL SENSITIVE	
IMTKS8.2	Reports for outside agencies – where the report has been included on the case file created by the outside agency		Whilst the child is attending the school then destroy				No	Yes	OFFICIAL SENSITIVE	
IMTKS8.3	Referral forms		While the referral is current then add to child's file				No	Yes	OFFICIAL SENSITIVE	
IMTKS8.4	Contact data sheets		Current year then review, if contact is no longer active then destroy				No	Yes	OFFICIAL SENSITIVE	
IMTKS8.5	Contact database entries		Current year then review, if contact is no longer active then destroy				No	Yes	OFFICIAL SENSITIVE	
IMTKS8.6	Group Registers		Current year + 2 years				No	Yes	OFFICIAL SENSITIVE	

Please note that the Family Liaison Officer records will not normally be shared with the head teacher without the consent of the parents. For more information please contact Michelle Hunt.