# JKHS DATA PROTECTION POLICY

## 1. Policy Statement

**1.1** This is the Data Protection Policy of John Kyrle High School and Sixth Form Centre.

**1.2** We are committed to processing Personal Information fairly and lawfully in accordance with the General Data Protection Regulation ("GDPR"), the Data Protection Act 2018 ("The DPA") and other related legislation which protects Personal Information. We recognise the importance of this and have updated our Policy to ensure that it gives effect to these important changes in the law.

**1.3** As a School, it is necessary for us to process Personal Information about our staff, pupils, parent(s) / guardian(s) and other individuals who we may come into contact with. In doing so, we recognise that the correct and lawful treatment of Personal Information is critical to maintaining the confidence of those connected with our School.

**1.4** This Policy has been updated to reflect our ongoing commitment to promoting a strong culture of data protection compliance in accordance with the law.

## 2. About this policy

**2.1** This Policy and any other documents referred to in it, sets out our approach to ensuring that we comply with data protection laws. It is critical that staff and trustees understand their responsibilities to handle personal information in accordance with the law and support that School in meeting its aim of maintaining a strong data protection culture.

**2.2** This policy does not form part of any employee's contract of employment and may be amended at any time.

**2.3** This policy has been approved by the Board of Trustees.

## 3. Definition of data protection terms

We have set out below some of the terms used in this policy along with a brief explanation about what they mean.

**3.1 Data Subjects** means an identified or identifiable natural person. For example, we process personal information about parents, staff members and pupils each of whom is a data subject.

**3.2 Personal Information** means any information about a data subject. Examples of personal information could include information about a pupil's attendance, medical conditions, Special Educational Needs requirements or photographs.

**3.3 Privacy Notices** are documents provided to data subjects which explain, in simple language, what information we collect about them, why we collect it and why it is lawful to do so. They also provide other important information which we are required to provide under data protection laws. See appendices 1, 2 and 3 for privacy notices.

**3.4 Data Controllers** determine the purpose and means of processing personal information. They are responsible for establishing practices and policies in line with the GDPR. The School is a 'Data Controller'.

**3.5 Data Users** are those of our staff members whose work involves processing personal information. Data users must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times.

**3.6 Processing** means when personal information is used in a particular way. For example, we may need to collect, record, organise, structure, store, adapt or delete personal information. When we do this, we will be 'Processing'.

**3.7 Special Category of Personal Information** means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health data, data concerning a data subject's sex life or sexual orientation. These types of personal information are regarded as being more 'sensitive' and the law requires increased safeguards to be in place if we are to process this type of data.

## 4. Data Protection Principles

**4.1** When we Process Personal Information, we will do so in accordance with the 'data protection principles'. In this regard, we will ensure that Personal Information is:-

(a) Processed lawfully, fairly and in a transparent manner **(Lawfulness, Fairness and Transparency)**.
(b) Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (**Data Minimisation**).
(d) Accurate and where necessary kept up to date (**Accuracy**).
(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (**Storage Limitation**).
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).

**4.2** We recognise that not only must we comply with the data protection principles, we must also demonstrate our compliance with these principles (**Accountability**).

## 5. Data Protection Officer

**5.1** The GDPR requires certain organisations, including schools, to appoint a 'Data Protection Officer' (DPO). The DPO must have expert knowledge in data protection law and practices. Our appointed DPO for the school who fulfils these requirements is from the Heart of Mercia, who can be contacted by email at dop@heartofmercia.com

The DPO will carry out a number of important tasks which will include:-

(a) monitoring compliance with data protection laws and our data protection polices, including managing internal data protection activities, raising awareness of data protection issues, training staff and conducting internal audits.
(b) advising on, and monitoring, data protection impact assessments.

(c) cooperating and being the first point of contact with the Information Commissioner's Office, members of staff, parents and pupils.

**5.2** The DPO will be independent of the School to avoid any conflict of interest.

**5.3** The DPO will report to the highest level of management in the School, which is to include the Headteacher and the Board of Trustees.

## 6. Lawfulness, fairness and transparency

### Lawful Processing

**6.1** Personal information must be processed lawfully. Under data protection laws, there are a number of grounds, which make it lawful to process personal information. We will only process personal information if one or more of the following apply:-

(a) the Data Subject has given his or her **consent**.
(b) the Processing is necessary for the **performance of a contract** with the Data Subject.
(c) the Processing is necessary to meet our **legal obligations**.
(d) the Processing is necessary to protect the Data Subject's **vital interests**.
(e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (often referred to as **Public Task**).

**6.2** We recognise that some categories of Personal Information are more sensitive and further conditions must be satisfied if we are to Process this information (Special category and criminal conviction data). Where we Process these categories of Personal Information, we will ensure that we do so in accordance with the additional conditions for Processing set out under the GDPR and the DPA.

### Consent

**6.3** Where it is necessary for us to obtain your consent to process personal information, we will ensure that we do so in accordance with data protection laws.

**6.4** Generally, we will only obtain consent where there is not another lawful ground (see 6.1) for Processing. Some examples as to when we will obtain your consent is if we want to place a photograph of a pupil in the newspaper, on social media or in other publications to celebrate their achievements.

**6.5** We recognise that under data protection laws, there are stricter rules as to how consent is obtained. We will ensure that when we obtain consent, we will:-

(a) take steps to ensure that we make it clear to Data Subjects what they are being asked to consent to.
(b) ensure that the Data Subject, either by a statement or positive action, gives their consent. We will never assume that consent has been given simply because a Data Subject has not responded to a request for consent.
(c) never use pre-ticked boxes as a means of obtaining consent.
(d) ensure that a Data Subject is informed that they can withdraw their consent at any time and the means of doing so.
(e) keep appropriate records evidencing the consents we hold.

### Transparency

**6.6** We are required to provide information to Data Subjects which sets out how we use their Personal Information as well as other information required by law. We will provide this information by issuing Privacy Notices which will be concise, transparent, intelligible, easily accessible, and in clear, plain language.

## 7. Processing for limited purposes

We will only collect and Process Personal Information for specified, explicit and legitimate reasons. We will not further Process Personal Information unless the reason for doing so is compatible with the purpose or purposes for which it was originally collected.

**8. Adequate, relevant and limited processing**

We will only collect Personal Information to the extent that it is necessary for the specific purpose notified to the Data Subject.

**9. Accurate data**

**9.1** We will ensure that Personal Information we hold is accurate and kept up to date.

**9.2** We will take all reasonable steps to ensure that Personal Information that is inaccurate is either erased or rectified without delay.

**9.3** In supporting the School to maintain accurate records, staff, parents and other individuals whose Personal Information we may Process are responsible for:-

(a) Checking that any information that they provide to the School is accurate and up to date; and

(b) Informing the School of any changes to information that they have provided.

**10. Retention**

**10.1** We will not keep Personal Information for longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy and erase from our systems, all data which is no longer required.

**10.2** We will maintain a records retention schedule which will assist the School to destroy Personal Information once it is no longer necessary and in a safe and secure manner.

**11. Individual rights**

**11.1** We will Process all Personal Information in line with a Data Subject's rights, in particular, their right to:

(a) Request **access** to any data held about them by the School.

(b) **Rectification** of inaccurate information.

(c) **Erasure** of Personal Information.

(d) **Restrict** the Processing of Personal Information.

(e) **Object** to the Processing of Personal Information.

(f) To receive Personal Information in a commonly used format (known as **data portability**) and have this transferred to another controller without hindrance.

**11.2** We will maintain a clear procedure detailing how such requests will be handled.

**12. Data security**

**12.1** We will implement appropriate technical and organisational measures to guard against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

**12.2** We will develop, implement and maintain safeguards appropriate to our size, scope, our available resources and the level of risk identified.

**13. Privacy by design and data protection impact assessments**

**13.1** We will integrate privacy by design measures when Processing Personal Information by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.

**13.2** We will utilise Data Protection Impact Assessments ("DPIAs") which will be used when introducing new technologies or the Processing is likely to result in a high risk to the rights and freedoms of Data Subjects.

## 14. Accountability

**14.1** As a Data Controller, we are responsible for, and must be able to demonstrate, compliance with the data protection principles. Examples of how we will demonstrate compliance include (but are not limited to):

(a) appointing a suitably qualified DPO
(b) implementing policies and procedures e.g., a data protection policy, data breach procedures and subject access procedures (see appendices 4 and 5)
(c) undertaking information audits and maintaining a record of our processing activities in accordance with Article 30 of the GDPR
(d) preparing and communicating Privacy Notices to Data Subjects
(e) providing appropriate training at regular intervals
(f) implementing privacy by design when Processing Personal Information and completing data protection impact assessments where Processing presents a high risk to the rights and freedoms of Data Subjects.

## 15. Disclosure and sharing of personal information

**15.1** Where it is necessary to share Personal Information outside of the school, we will inform you about this in accordance with this policy.

**15.2** Examples of who we may share Personal Information with include other schools, the Local Authority and the Department of Education.

## 16. Data breaches

All data breaches must be handled in accordance with the school's internal breach reporting procedure.

## 17. Changes to this procedure

We reserve the right to change this procedure at any time and notification of any changes will be communicated accordingly.

## 18. Links with other documents

- **Appendix 1 - Parent Privacy Notice 2024**
- **Appendix 2 - Students Privacy Notice 2024**
- **Appendix 3 - Workforce Privacy Notice 2024**
- **Appendix 4 - Data Breach Procedure**
- **Appendix 5 - Subject Access (SAR) Procedure**
- **Appendix 6 - Retention Schedule**

| | |
|---|---|
| Policy reviewed: | January 2024 |
| Change(s) made: | Updated DPO contact in policy and privacy notices |
| Reviewed by: | DPO – Heart of Mercia |
| Review date: | Spring term 2026 (bi-annual) |
| Approved by: | |

# Appendix 1: JKHS privacy notice relating to parent information

**What is the purpose of this Notice?**
This is our school's Privacy Notice which is intended to provide you with information about how and why we process parent information. It is also intended to provide you with other information which is required under the UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) (GDPR) and the Data Protection Act 2018 (DPA). The GDPR and DPA contain the key laws relating to data protection.

It is important to the school, and a legal requirement, that we are transparent about how we process parent information. As a school that processes parent information, we are known as a "data controller". This means that we collect and use personal information for specified purposes which this Privacy Notice has been designed to tell you about.

**The Data Protection Officer**
The Data Protection Officer (DPO) for the school can be contacted on dpo@heartofmercia.org.uk The DPO is responsible for dealing with data protection issues within the school and you can contact the DPO should you wish to discuss any issues or concerns that you have about data protection.

**What categories of parent information do we collect?**
The types of parent information that we collect include:

- Parent names
- Date of birth
- Unique National Insurance number
- Contact details
- CCTV images

We may also receive some information from our Local Authority, other schools and the DfE.

**What is the purpose of us collecting and using parent information?**
The purposes for which the school collects personal information are as follows:

- To communicate with parents/carers about their child
- Monitor and report on student process
- To provide appropriate pastoral care
- For health and safety purposes
- To address safeguarding concerns
- To receive government funding

**Why is it lawful to collect this parent information?**
As a school, we are subject to a wide range of laws which we must comply with, including maintaining contact with individuals with parental responsibility for our students. To comply with these laws, we only process personal information as far as is necessary to meet those obligations. We also process some of the information described in this privacy notice to carry out public tasks vested in us to effectively manage the school.

Some types of personal information are regarded as more sensitive under the GDPR and referred to as being a 'special category' of personal information. We are unlikely to process this type of information in relation to parents.

**Who will we share parent information with?**
Those who we may share parent information with include the following:-

- Our local authority
- The Department for Education (DfE)
- Other education providers

- Multi-agency partners
- Professional advisors
- Service providers who provide IT and communication tools

**The Department for Education**
The Department for Education (DfE) collected personal data from educational settings and local authorities via various statutory data collections. We are required to share information with the DfE either directly or via our local authority for the purpose of those data collections under Section 5 of The Education (Information About Individual Students) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see 'How government uses your data' section.

**Local Authorities**
We may be required to share information about our students with the local authority to ensure that they can conduct their statutory duties under the Schools Admission Code, including conducting Fair Access Panels.

**How long will we hold parent information for?**
We will hold parent information for a period of time specified by law and as detailed within our retention policy. For more information, please contact the DPO.

**Requesting access to your personal data**
Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information (a subject access request) please contact the school via admin@jkhs.org.uk to put your request in writing.

You also have the right 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,
- Claim compensation for damages caused by a breach of the Data Protection Regulations

**Making a complaint**
If you have a concern about the way we are collecting or using your personal data, you should raise your concern with the Data Protection Officer via email to dpo@heartofmercia.org.uk in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns

**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

| | |
|---|---|
| Document reviewed: | January 2024 |
| Reviewed by: | DPO – John Kyrle High School |
| Review date: | Spring term 2026 (bi-annual) |

# Appendix 2 - JKHS privacy notice for student information

**What is the purpose of this Notice?**
This is our school's Privacy Notice which is intended to provide you with information about how and why we process student information. It is also intended to provide you with other information which is required under the UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) (GDPR) and the Data Protection Act 2018 (DPA). The GDPR and DPA contain the key laws relating to data protection.

It is important to the school, and a legal requirement, that we are transparent about how we process student information. As a school that processes student information, we are known as a "data controller". This means that we collect and use personal information for specified purposes which this Privacy Notice has been designed to tell you about.

**The Data Protection Officer**
The Data Protection Officer (DPO) for the school can be contacted on dpo@heartofmercia.org.uk The DPO is responsible for dealing with data protection issues within the school and you can contact the DPO should you wish to discuss any issues or concerns that you have about data protection.

**What categories of student information do we collect?**
The types of student information that we collect include:

- Student names, unique student numbers, contact details including emergency contacts
- Characteristics such as ethnicity, language, religion.
- Free school meal and student premium eligibility
- Medical information and dietary requirements
- Admissions information
- Attendance information
- Information relating to student exclusion and behaviour
- Attainment records and assessment results
- Reported accidents
- Safeguarding information
- Special educational needs information
- Photographs
- CCTV
- Biometric data (fingerprints)
- Careers information

We may also receive some information from our Local Authority, other schools and the DfE.

**What is the purpose of us collecting and using student information?**
The purposes for which the school collects personal information are as follows:-

- To provide appropriate pastoral care
- Census reporting
- To provide free school meals
- To support children with medical conditions, allergies and SEN
- To manage admissions
- To monitor attendance
- To manage exclusions and behaviour
- For assessment and examination purposes
- For health and safety purposes
- To address safeguarding concerns
- To promote the school and celebrate educational achievement
- To ensure that the school is safe and secure
- To allow cashless payments to be made
- To provide careers advice and support

**Why is it lawful to collect this student information?**
As a school, we are subject to a wide range of laws which we must comply with to further student education and to safeguard their wellbeing. To comply with these laws, we only process personal information as far as is necessary to meet those obligations. We also process some of the information described in this privacy notice to carry out public tasks vested in us to effectively manage the school.

In limited circumstances, we will obtain your consent; for example, if we want to place photographs of students on our website, in the newspaper or on social media. Even if you consent to us collecting and using personal information, you have a right to withdraw your consent at any time.

Some types of student information are regarded as more sensitive under the GDPR and referred to as being a 'special category' of personal information. This could include information which we collect for safeguarding or SEN purposes. Where we process this type of personal information, it will often be processed for reasons of substantial public interest such as safeguarding or to comply with statutory requirements.

**Withdrawal of consent**
Where we are processing your personal data with your consent, you have the right to withdraw your consent at any time. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the school's Data Manager on 01989 764358 or via admin@jkhs.org.uk

**Who will we share student information with?**
Those who we may share student information with include the following:-

- Our local authority
- The Department for Education (DfE)
- Other education providers
- School nurse service
- Multi-agency partners
- Professional advisors
- Careers service providers
- Service providers who provide learning platforms, IT and communication tools

**Youth support services**
**Students aged 13+:**
Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can object to any information in addition to their child's name, address and date of birth being passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / student once they reach the age 16.

Data is securely transferred to the youth support service via a password protected secure email and is stored on the school's network and can only be accessed by those people who have responsibility for the information. The information is held for the current year and then reviewed.

**Students aged 16+:**
We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13 to 19 year-olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

A child / student once they reach the age of 16 can object to only their name, address and date of birth is passed to their local authority or provider of youth support services by informing us.

Data is securely transferred to the youth support service via password protected secure email and information is stored on the school's network and can only be accessed by those people who have responsibility for the information. The information is held for the current year and then reviewed.

For more information about services for young people, please visit our local authority website.

**The Department for Education**
The Department for Education (DfE) collected personal data from educational settings and local authorities via various statutory data collections. We are required to share information with the DfE either directly or via our local authority for the purpose of those data collections under Section 5 of The Education (Information About Individual Students) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see 'How government uses your data' section.

**Local Authorities**
We may be required to share information about our students with the local authority to ensure that they can conduct their statutory duties under the Schools Admission Code, including conducting Fair Access Panels.

**How long will we hold student information for?**
We will hold student information for a period of time specified by law and as detailed within our retention policy. For more information, please contact the DPO.

**Requesting access to your personal data**
Under data protection legislation, parents and students 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, please contact the school via email admin@jkhs.org.uk to request the details in writing.

You also have the right 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 laws.

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

**How Government uses your data**
The student data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Student Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

**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 Data collection and censuses for schools

**The National Student Database (NPD)**
Much of the data about students in England goes on to be held in the National Student Database (NPD). The NPD is owned and managed by the Department for Education and contains information about students 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.

To find out more about the NPD, go to Department for Education (DfE) personal data

**Sharing by the Department**
The law allows the Department to share students' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit:
Data protection - how we collect and share research data

Organisations fighting or identifying crime may use their legal powers to contact the DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 students per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided student information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: DfE external data shares

**How to find out what personal information DfE hold about you**
Under the terms of the Data Protection Act 2018, you are entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

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

| | |
|---|---|
| Document reviewed: | January 2024 |
| Reviewed by: | DPO – John Kyrle High School |
| Review date: | Spring term 2026 (bi-annual) |

# Appendix 3 - JKHS workforce inc trustees privacy notice

**What is the purpose of this Notice?**

This is our school's privacy notice which is intended to provide you with information about how and why we process your personal information. It is also intended to provide you with other information which is required under the UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) (GDPR) and the Data Protection Act 2018 (DPA). The GDPR and DPA contain the key laws relating to data protection.

It is important to the school, and a legal requirement, that we are transparent about how we process your personal information. As a school that processes personal information, we are known as a "data controller". This means that we collect and use personal information for specified purposes which this privacy notice has been designed to tell you about.

**The Data Protection Officer**

The Data Protection Officer (DPO) for the school can be contacted on dpo@heartofmercia.org.uk The DPO is responsible for dealing with data protection issues within the school and you can contact the DPO should you wish to discuss any issues or concerns that you have about data protection.

**What personal information do we collect?**

The types of personal information that we collect will include: -

- personal information (such as name, employee or teacher number, national insurance number, next of kin and contact details)
- special categories of data including characteristics information such as gender, age, ethnic group
- recruitment information
- contract information (such as start dates, hours worked, post, roles, subjects taught and salary information)
- work absence information (such as number of absences and reasons, annual leave and maternity leave)
- qualifications, subjects taught and training records
- performance information
- grievance and disciplinary information
- health and safety information (such as accidents at work)
- relevant medical information
- safeguarding information
- DBS information
- CCTV

**What is the purpose of us collecting your personal information?**

We process personal data relating to those we employ to work at, or otherwise engage to work at, our school. This is for employment purposes to assist in the running of the school and to enable individuals to be paid. The purpose for which we process workforce personal information include:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- managing the recruitment process
- carrying out pre-employment checks and equal opportunities monitoring
- complying with the terms of the contract of employment
- making reasonable adjustments
- enabling individuals to be paid
- managing absence
- managing performance, grievance and disciplinary matters
- safeguarding purposes
- managing workplace accidents

**Why is it lawful to collect this information?**
We process your personal information, but no more than is necessary, to comply with legal obligations which the school is subject to or because processing is necessary to comply with the terms and conditions of your contract of employment.

In limited circumstances, we may require your consent. If this is the case, we will inform you of the reasons that we need to process your personal information in accordance with the GDPR and DPA. You will be able to withdraw your consent at any time should you wish to do so.

Where we process sensitive personal information (special category data) we will usually do this, only as far as necessary, to comply with employment law obligations which we are subject to or because it is in the public interest to do so e.g., for safeguarding reasons.

**Who will we share this information with?**
We are required, by law, to pass on some of this personal data to:

- the Department for Education (DfE)
- HMRC

We may also share some information with: -

- the local authority
- health and safety executive
- DBS
- insurance providers
- training providers
- professional advisors
- IT and communications technology providers
- auditors

**How long will we hold your information for?**
We will hold personal information for a period specified within our retention policy. We generally hold school workforce personal information for the period of your employment until termination and a period of 6 years thereafter. For more information, please ask the DPO for a copy of our retention schedule.

**Department for Education (DfE)**
The DfE collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our school employees with the DfE under section 7 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework. For more information, please see 'How Government uses your data' section.

**Requesting access to your personal data**
Under data protection legislation, you have the right to request access to information that we hold. To make a request for your personal information please contact the school's DPO.

Depending on the lawful basis above, you may also have the right to:

- object to processing of personal data that is likely to, 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
- a right to seek redress, either through the ICO, or through the courts

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

For further information on how to request access to personal information held centrally by the DfE, please see 'How the Government uses your data' section of this notice.

**Withdrawal of consent and the right to lodge a complaint**
Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the DPO via email dpo@heartofmercia.org.uk

**How the Government uses your data**
The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of effectiveness and the diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy.

**Data collection requirements**
To find out more about the data collection requirements placed on us by the DfE including the data that we share with them, go to www.gov.uk/education/data-collection-and-censuses-for-schools

**Sharing by the department**
The Department may share information about school employees with third parties who promote the education or well-being of young people or the effective deployment of school staff in England by:

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

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment:

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

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

**How to find out what personal information the DfE hold about you**

Under the terms of the Data Protection Act 2018, you are entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they are holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the department: www.gov.uk/contact-dfe

| | |
|---|---|
| Document reviewed: | January 2024 |
| Reviewed by: | DPO – John Kyrle High School |
| Review date: | Spring term 2026 (bi-annual) |

# Appendix 4: JKHS Data Breach Procedure

## 1. Policy Statement

1.1 John Kyrle High School and Sixth Form Centre ("the School") processes a significant amount of personal information about its students, parents, staff, volunteers and other individuals who we come into contact with. This can include sensitive information ("Special Category Data").

1.2 By complying with our own internal data protection procedures, and through promoting a strong culture of data protection compliance, our aim is to avoid the occurrence of a data breach. However, we recognise that in the event of a data breach, it is critical that we have effective response procedures in place to minimise the impact on those affected.

1.3 The UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) ("GDPR") also places reporting obligations on the School, as a data controller, in the event of a data breach. This procedure has been implemented to ensure that appropriate action is taken in a timely manner to comply with the requirements of the GDPR.

1.4 This procedure applies to all school staff, trustees, volunteers and contractors.

## 2. Identifying a Data Breach

2.1 A data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. It is therefore important to recognise that a data breach is not just the loss of personal information.

2.2 Examples of data breaches include the following:

(a) Loss or theft of personal data and / or equipment on which data is stored.
(b) Sending personal information to the incorrect recipient.
(c) Unauthorised access of personal information.
(d) Hacking.
(e) Cyber-attack.
(f) Accidental destruction.

2.3 The above list is not exhaustive. If you are in any doubt as to whether a data breach has occurred or not, you should err on the side of caution and report it in accordance with this procedure.

## 3. Reporting the Breach and Immediate Steps

3.1 Any person who has personally caused a data breach, discovers a data breach, or is informed of the occurrence of a data breach, must immediately notify the school via telephone 01989 764358 or email admin@jkhs.org.uk Alternatively the Data Protection Officer (DPO) for the Heart of Mercia MAT should be notified directly via email dpo@heartofmercia.org.uk

3.2 The school must immediately report the data breach to the DPO by emailing dpo@heartofmercia.org.uk

3.3 If, in the opinion of the DPO, the data breach is likely to result in a risk to the rights and freedoms of those affected, the Chair of Trustees should be notified.

3.4 The DPO will be responsible for assessing the data breach and advising the school on any immediate action that it may need to take to address any risks arising. In doing so, the DPO will consider the following:

(a) Is the data breach still occurring?
(b) If the answer to (a) is yes, then immediate steps must be agreed to minimise the breach from continuing.
(c) Consideration should be given to notifying the police if the breach was caused by, or suspected to have been caused by, unlawful activity (e.g., hacking). The police should also be notified if the breach may lead to unlawful activity in the future (e.g., if bank details have been lost in human error, this could lead to fraud in the future).
(d) Any third parties who may be affected by the breach should be notified. This could include the relevant local authority departments (e.g., Children Services) and service providers.

(e) If the nature of the breach is such that it may result in media or press enquiries, those responsible for handling such enquiries should be notified. The DPO will also assist with any information to be provided to the media.
(f) ICT technicians at the school and / or third-party ICT providers should be consulted, if appropriate, to advise on any security measures that can be put in place to minimise the impact of the breach e.g. shutting down systems, changing passwords, retrieving lost data.
(g) Where bank details have been lost or stolen, banks should be contacted to assist them in responding to any potentially fraudulent activity.

**4. Investigation**

4.1 The DPO must immediately support the school in investigating the data breach reported, taking such steps as are reasonable to identify the following:
a) When the breach occurred.
b) The factual background relating to the breach.
c) Who has been affected by the breach e.g. staff, parents or students?
d) The number of people affected by the breach.
e) The type and sensitivity of the data concerned.
f) The consequences or potential consequences of the breach.
g) The measures put in place to minimise the breach.

4.2 The investigation should be completed urgently as its findings will inform whether the Information Commissioner's Office ("ICO") and/or data subjects need to be informed.

**5. Record of Breach**

The DPO must record the data breach in the Data Breach Record.

**6. Notification of a Data Breach to the ICO**

6.1 Subject to 6.3, the DPO will ensure that a data breach is reported to the ICO not later than 72 hours after the School became aware of the breach using the telephone service or the online ICO report form.
6.2 Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.
6.3 If the data breach is unlikely to result in a risk to the rights and freedoms of those affected by the breach, then the notification to the ICO described at 6.1 will not be necessary.
6.4 A data breach is likely to result in a risk to the rights and freedoms of those affected by the breach if it causes a loss of control over their personal information or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality. These examples are not exhaustive, and the breach must be assessed on a case-by-case basis by the DPO.
6.5 If a notification to the ICO is made, the DPO will ensure that appropriate steps are taken to fully co-operate with their requests / investigations.

**7. Notifying the Data Subject(s)**

7.1 Subject to 7.2, if the data breach is likely to result in a high risk to the rights and freedoms of the data subject(s) the DPO will ensure that steps are taken by the School to notify the data subjects without delay using the letter template at form A.
7.2 Those affected by the data breach need not be notified if any of the following apply:
(a) The School had implemented appropriate technical and organisational measures, and those measures were applied to the personal information affected by the data breach, in particular, those that ensure

the personal information is unintelligible to any person who is not authorised to access it, such as encryption and the data is recoverable e.g. as it was backed-up.

(b) The School has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.

## 8. Post Breach Procedure

8.1 It is imperative that regardless of how serious or minor the breach, lessons are learnt, and measures are put in place to avoid a similar incident occurring again in the future.

8.2 The measures put in place should be proportionate to the breach. However, such measures could include the provision of further training, introduction of new policies and procedures or changes to security measures.

8.3 Where the breach was notified to the Chair of Trustees in accordance with 3.2, the Headteacher will report the findings of the investigation at the next Trustees meeting including the measures introduced to avoid any future breaches.

| | |
|---|---|
| Document reviewed: | January 2024 |
| Reviewed by: | DPO – John Kyrle High School |
| Review date: | Spring term 2026 (bi-annual) |

**FORM A**

[Name]
[Insert Address 1]
[Insert Address 2]
[Insert Postcode]

[Date]

Dear XXXX

**Notification of a Data Breach**

We write to advise you of a recent data breach within the school. Having considered the nature of the breach, we have reported this to the Information Commissioner's Office who will advise us of the next steps in their process. The ICO is the UK's independent body set up to uphold information rights.

The purpose of this letter is to provide you with information about the data breach, how it occurred, who it has affected, the type of information which the breach relates to, the consequences of the breach and the measures we have taken to address the breach.

**Details of the breach**
[INSERT DETAIL]

**Name and contact details of the Data Protection Officer**
We have an appointed data protection officer who is actively working with the school to address the data breach and their contact details are as follows:
Heart of Mercia
Hereford College
Folly Lane
Hereford
HR1 1LU
dpo@heartofmercia.org.uk

**The likely consequences of the data breach**
[INSERT DETAIL]

**Measures taken or proposed to be taken by the School to address the data breach**
[INSERT DETAIL]

Clearly, we appreciate that you will be concerned about the data breach described within this letter. On behalf of the school, we sincerely apologise for any distress that this may cause. We can assure you that we are taking all necessary steps to address the situation. Should you wish to discuss this with the DPO, then please feel free to do so by emailing dpo@heartofmercia.org.uk

Yours sincerely,

For and on behalf of John Kyrle High School and Sixth Form Centre

# Appendix 5: JKHS Subject Access (SAR) Procedure

**Policy Statement**

This is the subject access procedure of John Kyrle High School & Sixth Form Centre ("the School"). We are committed to complying with requests for information, and respecting individual rights set under the UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) (GDPR) and the Data Protection Act 2018 (DPA), and other laws and regulations which create important individual rights.

**Application of this procedure**

Parents, pupils, staff and other individuals who we process personal data about are entitled to access, subject to certain exceptions, the personal data which we hold about them.

When the School receives a request for personal information, it is important that this procedure is followed.

**Subject Access Procedure**

1. Under the GDPR, individuals such as pupils, parents and staff are entitled to access personal data which we hold about them. The GDPR also sets out when such requests may be refused.
2. A subject access request should be made in writing to the Business and Finance Director.
3. On receipt of a subject access request, we will send a letter or email to the requester acknowledging receipt.
4. We will take steps to verify the identity of the requester, and where a parent requests personal data relating to their child, proof of their relationship to the child. We may require the requester to provide proof of identity, such as a passport, driving licence and / or the child's birth certificate. This is a security measure to ensure that we only disclose personal data to those who are entitled to receive it.
5. Where the request is received from a pupil or former pupil then, as a general rule, if they are aged 13 or older, we will deem them to be able to understand the request that they are making. However, If the child cannot understand the nature of the request, someone with parental responsibility may ask for the information on the child's behalf. All requests will be dealt with on a case-by-case basis and the DPO should be consulted where appropriate.
6. We will respond to subject access requests as soon as possible, but in any event no later than 1 month from the receipt of the request subject to paragraph 6.
7. If the nature of the request is complex, or there are other legitimate reasons for doing so, we may, if necessary, extend the period under paragraph 5 for up to 2 months. If we require an extension of time of over 1 month to deal with a subject access request, we will inform the requester as soon as possible, but in any event no later than 1 month from the date that the request was made.
8. Before providing the information requested, we will review it to identify whether it contains any information relating to other individuals. Where other individuals are named, such as pupils, then we will redact this data to ensure that they are not identifiable. Generally, references to teacher names will not be redacted.
9. Where the personal data has been provided by another agency, such as the Police, Local Authority, Health Care professionals or another school we will obtain their consent first before disclosure.

**Exemptions to the subject access procedure**

1. We will not charge a fee for responding to subject access requests unless the request, in the opinion of the school, is unfounded, excessive and/or repetitive.
2. There are some exemptions to the right of access that apply in certain circumstances or to certain types of personal data. Therefore, all information must be reviewed prior to disclosure. The exemptions include the following: -

a) Personal data processed by a court and consisting of information supplied in a report or other evidence given to the court in the course of proceedings.
b) Personal data where the disclosure would be likely to cause serious harm to the physical or mental health or condition of the pupil or any other person.
c) Information as to whether the pupil is, or has been the subject of, or may be at risk of child abuse if disclosure would not be in their best interests. “Child abuse data” is personal data consisting of information as to whether the pupil is or has been the subject of, or may be at risk of, child abuse.

3. If there are concerns over the disclosure of information, then additional advice should be sought from the DPO.

**Additional Rights**

4. Where an individual seeks to exercise additional rights such as the following: -
   a) Right to rectification
   b) Right of Erasure
   c) Right of objection
   d) Right to restrict processing
   e) Right to data portability.

The DPO should be consulted immediately who will advise on the correct procedure to be followed.

**Complaints**

Complaints about this procedure should be made using the school’s Complaints Policy, where a copy can be found on the school’s website under the section About Us > Polices.

Complaints which are not appropriate to be dealt with through the School’s complaint procedure can be dealt with by the Information Commissioner’s Office. Contact details of both will be provided with the disclosure information.

# Appendix 6 – Education retention schedule

## Contents


1. Pupil records Page 2
2. School trips and extra-curricular activities Page 3
3. Teaching and curriculum Page 3
4. Staff, health and safety, payroll and financial records Page 4
5. Safeguarding Page 6
6. Central government and local authority Page 6
7. Governing body records Page 7

# Retention schedule

## 1. Pupil records

| PR | Basic file description | Justification | Retention Period |
|---|---|---|---|
| **PR 1** | **Admissions and Attendance** | | |
| PR 1.1 | Admission Registers | Common Practice | Permanent |
| PR 1.2 | Records relating to the admissions process if the admission is successful | Common Practice | Admission + 1 year |
| PR 1.3 | Records relating to the admissions process if the appeal is unsuccessful | The School Admission Appeals Code issued under Section 84 of the School Standards and Framework Act 1998 | Conclusion of the appeal process + 1 year |
| PR 1.4 | Attendance registers | Common Practice | Date of register + 3 years |
| PR 1.5 | Parent declaration form for nursery education funding | Common Practice | Date funding ceases + 6 years |
| **PR 2** | **Pupil Educational Record** | | |
| PR 2.1 | Pupil Files – Primary School | Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437) | Retain for the time which the pupil remains at the Primary School then transfer to the Secondary School (or other Primary School) when the child leaves the school |
| PR 2.2 | Pupil Files Secondary | Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437) | DOB of the pupil + 25 years |
| PR 2.3 | Examination results - Public | Common Practice | Year of examinations + 6 years |
| PR 2.4 | Examination results - Internal examination results | Common Practice | Current year + 5 years |
| PR 2.5 | Images held of pupils together with any consents and permissions to publish | Common Practice | All records relating to the image should be retained for the period that the consent is in place. |
| **PR 3** | **Special Educational Needs** | | |
| PR 3.1 | Special Educational Needs files, reviews and Individual Education Plans | Common Practice | DOB of the pupil + 25 years<br>Unless legal action is pending |
| PR 3.2 | Statement maintained under The Education Act 1996 - Section 324 | Common Practice | DOB + 25 years<br>Unless legal action is pending |
| PR 3.3 | Proposed statement or amended statement | Special Educational Needs and Disability Act 2001 Section 1 | DOB + 25 years<br>Unless legal action is pending |
| PR 3.4 | Advice and information to parents regarding educational needs | Special Educational Needs and Disability Act 2001 Section 2 (now repealed) | Closure + 12 years<br>Unless legal action is pending |

## 2. School trips and extra-curricular activities

| ST | Basic file description | Statutory Provisions | Retention Period |
|---|---|---|---|
| **ST 1** | **Trips** | | |
| ST 1.1 | Parental permission slips for school trips – where there has been no major incident | Common Practice | Conclusion of the trip |
| ST 1.2 | Parental permission slips for school trips – where there has been a major incident | Common Practice | DOB of the pupil involved in the incident + 25 years. The permission slips for all pupils on the trip need to be retained in these circumstances |

## 3. Teaching and curriculum

| SMT | Basic file description | Statutory Provisions | Retention Period |
|---|---|---|---|
| **SMT 1** | **Senior Management Team** | | |
| SMT 1.1 | Log-Books | Common Practice | Date of last entry in the book + 6 years |
| SMT 1.2 | Minutes of the Senior Management Team | Common Practice | Date of meeting + 5 years |
| SMT 1.3 | Reports made by the Head Teacher or the management team | Common Practice | Date of report + 3 years |
| SMT 1.4 | Records created by Head Teachers, Deputy Head Teachers, Heads of Year and other members of staff with administrative responsibilities | Common Practice | Current academic year + 6 years |
| SMT 1.5 | School development plans | Common Practice | Expiry of plan + 6 years then review |
| SMT 1.6 | Professional development plans | Common Practice | Expiry of plan + 6 years |
| **SMT 2** | **Curriculum Management** | | |
| SMT 2.1 | Timetable | Common Practice | Current year then review |
| SMT 2.2 | Curriculum development | Common Practice | Current year + 6 years |
| SMT 2.3 | Curriculum returns | Common Practice | Current year + 3 years |
| SMT 2.4 | School syllabus | Common Practice | Current year then review |
| SMT 2.5 | Schemes of work | | Current year then review with a view to destroy |
| SMT 2.6 | Class record books | | Current year then review with a view to destroy |
| SMT 2.7 | Mark Books | | Current year then review with a view to destroy |

| SMT | Basic file description | Statutory Provisions | Retention Period |
|---|---|---|---|
| SMT 2.8 | Record of homework set | | Current year then review with a view to destroy |
| SMT 2.9 | Pupils' work | | Current year then review with a view to destroy |

## 4. Staff / health and safety / payroll and financial records

| HR | Basic file description | Statutory Provisions | Retention Period |
|---|---|---|---|
| **HR 1** | **Personnel Management** | | |
| HR 1.1 | Staff Personnel files | Limitation Act 1980 | Termination + 6 years |
| HR 1.2 | Interview notes and recruitment records | Justification based on time limits issue for issuing proceedings in the employment tribunal | Date of interview + 9 months |
| HR 1.3 | Pre-employment vetting information (including DBS checks) | DBS guidelines | Date of check + 6 months |
| HR 1.4 | Right to Work in the UK checks | https://www.gov.uk/check-job-applicant-right-to-work | Termination of employment + 2 years |
| HR 1.5 | Written particulars of employment.<br>Contracts of employment or other contracts.<br>Documented changes to terms and conditions. | Limitation Act 1980 | Termination + 6 years |
| HR 1.6 | Disciplinary and grievance records | Limitation Act 1980 | Termination + 6 years |
| HR 1.7 | Annual appraisal or assessment records | Common Practice | Current year + 5 years |
| HR 1.8 | Images held of members of staff together with any consents and permissions to publish | Common Practice | 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 in the consent. |
| **HR 2** | **Health and Safety** | | |
| HR 2.1 | Accessibility Plans | Equality Act 2010 (See s.88 and schedule 10) | Current year + 6 years |
| HR 2.2 | Records relating to accident/injury at work | The Management of Health & Safety at Work Regulations 1999<br>Health and Safety at Work Act 1974 | Date of incident + 12 years [1] |
| HR 2.3 | Accident Reporting – Children | Limitation Act 1980 | Date of birth + 22 years where the injured person is a minor at the time of the accident |

| HR | Basic file description | Statutory Provisions | Retention Period |
|---|---|---|---|
| HR 2.4 | Accident Reporting – Adults | Social Security (Claims and Payments) Regulations 1979 Regulation 25.<br>Social Security Administration Act 1992 Section 8.<br>Limitation Act 1980 | Date of the accident + 4 years where the injured person is an adult at the time of the accident; |
| HR 2.5 | Risk Assessments | The Management of Health & Safety at Work Regulations 1999<br>Health and Safety at Work Act 1974 | Current year + 3 years |
| HR 2.6 | COSHH Risk Assessments | Control of Substances Hazardous to Health (COSHH) Regulations 2002 | Date of creation + 40 years |
| HR 2.7 | Incident reports | | Current year + 20 years |
| HR 2.8 | 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 |
| HR 2.9 | 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 |
| HR 2.10 | Fire Safety Records including Fire Safety Audits | Regulatory Reform (Fire Safety) Order 2005 | Current year + 6 years |
| HR 2.11 | Fire Risk Assessments | Regulatory Reform (Fire Safety) Order 2005 | Date the fire risk assessment expires + 6 years |
| HR 2.12 | Fire Drill records | Regulatory Reform (Fire Safety) Order 2005 | Date of fire drill + 6 years |
| **HR 3** | **Payroll and Pensions** | | |
| HR 3.1 | Records relating to the management of the payroll | HMRC - Compliance Handbook Manual CH15400 | Financial year to which the payroll is run + 6 years |
| HR 3.2 | Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995 | Retirement Benefits Schemes (Information Powers) Regulations 1995 | Current year + 6 years |
| HR 3.3 | Salary cards | | Last date of employment + 85 years |
| HR 3.4 | Maternity pay records | Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567) | Current year + 3yrs |
| HR 3.5 | Timesheets, sick pay | | Current year + 6 years |
| **HR 4** | **School Meals** | | |
| HR 4.1 | Dinner Register | | Current year + 3 years |
| HR 4.2 | School Meals Summary Sheets | | Current year + 3 years |
| HR 4.3 | Free school meals registers | HMRC - Compliance Handbook Manual CH15400 | Current year + 6 years |

| HR 5 | General Administration | | |
|---|---|---|---|
| HR 5.1 | School brochure/prospectus | | Current year + 3 years |
| HR 5.2 | General file series or correspondence files | | Current year + 5 years |
| HR 5.3 | Circulars (staff/parents/pupils) | | Current year + 1 year |
| HR 5.4 | Newsletters, ephemera | | Current year + 1 year |
| HR 5.5 | Visitors book | | Current year + 2 years |
| HR 5.6 | 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 |
| HR 5.7 | Records relating to the management of PTA/Old Pupils Associations | | Current year + 6 years |
| HR 5.8 | Records relating to the management of data subject access requests | | Current year + 3 years |
| HR 5.9 | Records relating to the management of freedom of information requests | | Current year + 3 years |

## 5. Safeguarding

| SG | Basic file description | Statutory Provisions | Retention Period |
|---|---|---|---|
| **SG 1** | | | |
| SG 1.1 | Child protection files (primary) | Published statutory guidance | Transfer to next school |
| SG 1.2 | Child protection files (secondary) | Published statutory guidance | DOB + 25 years |
| SG 1.3 | Allegations of a child protection nature made against a member of staff (including unfounded allegations) | Common Practice | Retain until the normal retirement age for the member of staff or for 10 years (whichever is the longer) |

## 6. Central government and local authority

| CG | Basic file description | Statutory Provisions | Retention Period |
|---|---|---|---|
| **CG 1** | **Local Authority** | | |
| CG 1.1 | Secondary transfer sheets (Primary) | Common Practice | Current year + 2 years |
| CG 1.2 | Attendance returns | Common Practice | Current year + 1 year |

| CG | Basic file description | Statutory Provisions | Retention Period |
|---|---|---|---|
| CG 1.3 | Circulars from LA | Common Practice | Whilst required operationally then review to see whether a further retention period is required |
| **CG2** | **Central Government** | | |
| CG 2.1 | OFSTED reports and papers | Common Practice | Replace former report with any new inspection report then review to see whether a further retention period is required |
| CG 2.2 | Returns | Common Practice | Current year + 6 years |
| CG 2.3 | Circulars from DfE | Common Practice | Whilst operationally required then review to see whether a further retention period is required |

## 7. Governing body records

| GB | Basic file description | Justification | Retention Period |
|---|---|---|---|
| **GB 1** | **Management of Governing Body** | | |
| GB 1.1 | Instruments of Government | Common practice | Permanent |
| GB 1.2 | Trusts and Endowments | Common practice | Permanent |
| GB 1.3 | Records relating to the election of parent and staff governors not appointed by the governors | To address any challenge to the election process | Date of election + 6 months |
| GB 1.4 | Records relating to the appointment of co-opted governors | Common practice | 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 |
| GB 1.5 | Records relating to the election of chair and vice chair | To address any challenge to the election process | Once the decision has been recorded in the minutes, the records relating to the election should be destroyed after 6 months. |
| GB 1.6 | Agendas – Principal copy | The School Governance (Roles, Procedures and Allowances) (England) Regulations 2013 (see Regulation 15) | Permanent |
| GB 1.7 | Minutes - Principal set (signed) | The School Governance (Roles, Procedures and Allowances) (England) Regulations 2013 (see Regulation 15) | Permanent |
| GB 1.8 | All records relating to the conversion of schools to Academy status | Common Practice | Permanent |
| GB 1.9 | Records relating to complaints made to and investigated by the Governing Body | Management of legal challenge | Date of resolution of complaint + 6 years then review for further retention in the case of contentious disputes |
| GB 1.10 | Correspondence sent and received by the Governing Body | Management of legal challenge | Current year + 6 years |

| GB 2 | Management of Governors | | |
|---|---|---|---|
| GB 2.1 | Records relating to the appointment of a clerk to the Governing Body | Common Practice | Date appointment as clerk ceases + 6 years |
| GB 2.2 | Records relating to the terms of office of serving governors including evidence of appointment | Common Practice | PERMANENT |
| GB 2.3 | Records relating to Governor Declaration against disqualification criteria | Common Practice | Until the Governor steps down |
| GB 2.4 | Register of Business Interests | Common Practice | PERMANENT |
| GB 2.5 | Records relating to the training required and received by Governors | Common Practice | Until the Governor steps down |
| GB 2.6 | Records relating to the induction programme for new governors | Common Practice | Until the Governor steps down |
| GB 2.7 | Records relating to DBS checks carried out on clerk and members of the governing body | Common Practice | Date of DBS check + 6 months |