



DATA PROTECTION POLICY

Reviewing Member of Staff: Mr B Freeman / Mrs M Wall

Date Updated: 06/02/2026

Date Approved by Governors: 05/03/2026

Review Date: Spring Term 2027

Committee: Safeguarding, Risk, Finance, Estates & General Purposes

Contents

Contents	2
1. Aims.....	3
2. Legislation and Guidance	3
3. Definitions	3
4. The Data Controller	4
5. Roles and Responsibilities	4
6. Data Protection Principles.....	5
7. Collecting Personal Data.....	5
8. Sharing Personal Data	6
9. Subject Access Requests and Other Rights of Individuals	6
10. Parental Requests to See the Educational Record	8
11. Biometric Recognition Systems	8
12. CCTV	8
13. Photographs and Videos	9
14. Data Protection by Design and Default	9
15. Data Security and Storage of Records	9
16. Data Retention and Disposal of Records	10
17. Personal Data Breaches	10
18. Training	10
19. Monitoring arrangements.....	11
20. Links with other policies	11
Appendix 1: Personal Data Breach Procedure	12
Appendix 2: Privacy Notice - Students	15
Appendix 3: UK GDPR Retention and Disposal of Records.....	Error! Bookmark not defined.

1. Aims

Prince Henry's High School Academy Trust (Prince Henry's) aims to ensure that all Personal Data collected about staff, students, parents/carers, Governors, Members, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(UK GDPR\)](#) and the provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Act 2018](#).

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

2. Legislation and Guidance

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#) and the ICO's [code of practice for subject access requests](#).

In addition, this Policy:

- Meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to Prince Henry's use of biometric data
- Reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information, and
- 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 individuals: • 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	Some Personal data is more sensitive, and so needs more protection, including information about an individual: • 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

Prince Henry's processes personal data relating to parents/carers, students, staff, Governors, Members, visitors and others, and is therefore a Data Controller. Prince Henry's is registered as a Data Controller with the ICO and renews this registration annually or as otherwise legally required.

5. Roles and Responsibilities

This policy applies to **all staff** employed by Prince Henry's, and to external organisations or individuals working on our behalf, including Governors and Members. Staff, Governors and Members who do not comply with this policy may face disciplinary action.

5.1 Governing Body (GB)

Whilst the Governing Body has overall responsibility for ensuring that Prince Henry's complies with all relevant data protection obligations, the Audit and Risk committee of the GB works with the Prince Henry's Data Protection Officer (DPO) to monitor Prince Henry's compliance with relevant data protection obligations, and to regularly report on Data Protection matters to the Governing Body.

5.2 Data Protection Officer (DPO)

Prince Henry's Data Protection Officer (DPO) is responsible for:

- Overseeing the implementation of this policy
- Informing and advising Prince Henry's and its employees about their obligations to comply with UK GDPR
- Monitoring Prince Henry's compliance with data protection law
- Developing related policies and guidelines where applicable
- Acting as the first point of contact for the ICO and individuals whose data is processed by the school

The DPO is required to provide, as a minimum, an Annual Report of their activities to the Governing Body and, where relevant, to provide the Governing Body with their advice and recommendations regarding Data Protection issues.

The DPO is the first point of contact for individuals whose data Prince Henry's processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

Within Prince Henry's, the DPO role is fulfilled by the Senior Support Staff Manager, who is contactable via secretary@princehenrys.worcs.sch.uk.

5.3 Operational Representatives of the Data Controller

The DPO will act as the representative of the Data Controller for their school on a day-to-day basis.

5.4 All Staff, Governors and Members

Staff, Governors and Members are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing Prince Henry's of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use Personal Data in a particular way
- If they need to rely on or capture consent, draft a Privacy Notice, deal with data protection rights invoked by an individual, or transfer Personal Data outside the European Economic Area
- If there has been, or they suspect that there may have 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 Prince Henry's 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 Prince Henry's aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, fairness and transparency

Prince Henry's will only process Personal Data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Prince Henry's can **fulfil a contract** with the individual, or the individual has asked Prince Henry's to take specific steps before entering into a contract
- The data needs to be processed so that Prince Henry's 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 Prince Henry's, 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 Prince Henry's 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 student) has freely given clear **consent**

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

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

7.2 Limitation, minimisation and accuracy

Prince Henry's 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, Governors and Members must only process Personal Data where it is necessary in order to do their jobs. When staff, Governors and Members no longer need the Personal Data they hold, they must ensure it is securely

deleted or anonymised. This will be done in accordance with the [Information and Records Management Society's Toolkit for Schools](#).

8. Sharing Personal Data

Prince Henry's will not normally share Personal Data with anyone else, but may do so where:

- There is an issue with a student or their parent/carer that puts the safety of our staff at risk
- There is an issue with a student, parent/carer, member of staff, Governor or Member that puts the safety of another individual or individuals at risk
- We need to liaise with other agencies - we will seek consent as necessary before doing this
- There is a need to share such information with a Third-Party Educational Service Provider (e.g. the providers of educational applications) in order to be able to undertake our obligation to provide education. We will always ensure that all such Third-Party Education Service Providers are UK GDPR compliant.
- Our suppliers or contractors need data to enable us to provide services to our staff and students - for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any Personal Data we share
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share Personal Data with law enforcement and Government bodies where we are legally required to do so, including for:

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

We may also share Personal Data with emergency services and Local Authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer Personal Data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law. Transfers are made in line with UK adequacy decisions or approved safeguards.

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 Prince Henry's holds about them. This includes:

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

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

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

If staff, Governors, Members receive a Subject Access Request they must immediately forward it to the DPO for their action within the required timescales.

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 aged 13 and above are generally 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 students at Prince Henry's aged 13 and above may not be granted without the express permission of the student. This is not a rule and a student'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 Subject Access Requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will acknowledge receipt of the request without delay and will endeavour to respond to the request within 1 month of receipt of the request
- In exceptional circumstances we may tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month of receipt of their request, and will explain why the extension is necessary
- Will provide the information free of charge

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

A Subject Access Request may be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

If Prince Henry's refuses a Subject Access 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, where their consent is required
- Ask us to rectify, erase or restrict processing of their Personal Data, or object to the processing of it (in certain circumstances)
- Prevent use of their Personal Data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their Personal Data is transferred outside of the European Economic Area

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a Data Breach in certain circumstances
- Make a complaint to the ICO
- Ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO.

If staff, Governors or Members receive such a request, they must immediately forward it to the DPO for their action.

10. Parental Requests to See the Educational Record

As an Academy, there is no automatic parental right of access to educational records. However, we will decide on a case-by-case basis whether or not to provide requested educational records within 15 school days of receipt of a written request, subject to the student, giving their consent to any such a request.

11. Biometric Recognition Systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it.

Prince Henry's will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use Prince Henry's biometric systems. We will provide alternative means of accessing the relevant services for those students.

Parents/carers and students can object to participation in Prince Henry's biometric recognition systems, or withdraw consent at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members or other adults use Prince Henry's biometric systems, we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and Prince Henry's will delete any relevant data already captured.

12. CCTV

We may elect to use CCTV in various locations around the school site in order to ensure the school remains safe. Where we use CCTV we will adhere to the ICO's [code of practice](#) for the use of CCTV.

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

Any enquiries about the usage of CCTV within the school should be directed to the Chief Operating Officer, who can be contacted via the school's main enquiries@princehenrys.worcs.sch.uk email address.

13. Photographs and Videos

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

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. We will obtain written consent from parents/carers of students aged under 18. We will obtain written consent directly from any students or other adults (e.g. staff, Governors) aged 18 and over, for photographs and videos to be taken for communication and/or marketing purposes.

Where we do not need parental consent, we will clearly explain to the student and/or the member of staff, Governor or Member how the photograph and/or video will be used. Uses may include:

- Within school on noticeboards and in school magazines, brochures, newsletters, etc.
- In school management systems used to store and process data, e.g. SIMS
- Outside of the school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school websites or social media pages

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

When using photographs and videos for marketing or promotional purposes we will not accompany them with any other personal information about the child or the individual, to ensure they cannot be identified.

14. Data Protection by Design and Default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing Personal Data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see Section 6)
- Completing privacy impact assessments where Prince Henry'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, Governors on data protection law, this policy, any related policies and any other data protection matters. We will also keep a record of attendance at such training
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all Personal Data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data Security and Storage of Records

Prince Henry's 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 must be kept securely when not in use.
- All Personal Data (e.g. student performance data) that is stored on portable electronic devices must be stored on an encrypted drive or device.

- Papers containing confidential personal data must not be left on office or classroom desks, on staffroom tables, pinned to publicly accessible and unsupervised notice/display boards, or left anywhere else where there is general access
- Where personal information, such as parental contact details or a student's medical details, needs to be taken off site, staff must sign this information in and out from school offices
- Passwords which conform with the school's ICT Acceptable Use Policy must be used to access computers, laptops and other electronic devices. Staff and students will be required to change their passwords at regular intervals
- Encryption software must be used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students, Governors who store personal information on their personal devices must follow the same security procedures as for equipment owned by Prince Henry's
- Where we need to share Personal Data with a third party, we will carry out due diligence and take reasonable steps to ensure such Personal Data is stored securely and is adequately protected (see Section 8)

16. Data Retention and Disposal of Records

Prince Henry's will retain students' educational records (e.g. relating to Admissions and Attainment) until they have attained the age of 25, or until the record has been passed on to another educational establishment.

Prince Henry's will retain all other records (e.g. Staff Records, Governing Body records) for 7 years after the individual has left Prince Henry's.

Safeguarding records are archived by the school electronically through the CPOMS Safeguarding System.

Personal Data that is no longer needed will be disposed of securely. Personal Data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records and overwrite or delete electronic files.

We may elect to 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.

17. Personal Data Breaches

Prince Henry's will make all reasonable endeavours to ensure that there are no Personal Data Breaches.

In the unlikely event of a suspected or actual Data Breach, we will follow the procedure set out in Appendix 1.

We will report any Data Breach, or suspected Data Breach, to the ICO within 72 hours of becoming aware of the breach or suspected breach. Such breaches may include, but are not limited to:

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

18. Training

All staff and Governors will be provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development for staff, Governors and Members, where changes to legislation, guidance or the Trust's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every year**, or more frequently if such a review is deemed necessary, and the findings of the review will be shared with the full Governing Body.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of Information Publication Scheme
- Safeguarding Policy
- ICT Acceptable Use (Staff & Governors) Policy

Appendix 1: Personal Data Breach Procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether Personal Data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO will alert the Headteacher, and if necessary, depending on the severity of the breach, the Chair of the Board.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO. Should there be any doubt, the DPO will seek the advice of the ICO's advice line and/or the school's legal advisers.

- 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 will be stored securely in the DPO's office.
- 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 being notified of the breach or suspected 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 being notified of the breach or suspected 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
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose Personal Data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the Personal Data Breach
 - A description of the measures that have been, or will be, taken to deal with the Data Breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals - for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored securely in the DPO's office.

- 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

Prince Henry's 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
- Students, Members of staff, Governors or Members who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the relevant ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure a written response is received from all the individuals who received the data, confirming that they have complied with the request to delete the information and not to share, publish, save or replicate it in any way
- 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

Sensitive information being disclosed via post (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via correspondence sent by post to an unauthorised individual, the sender must inform the DPO and attempt to recover the correspondence as soon as they become aware of the error
- The DPO will establish the reason for the correspondence being sent to an unauthorised individual and, if this is due to incorrect information (for example, address details) being held on file, ensure that contact details are correctly updated and that incorrect details are removed
- If the sender is unable to recover the correspondence, the DPO will endeavour contact the relevant unauthorised individuals who received the correspondence, explain that the information was sent in error, and request that those individuals return the correspondence to the school, and do not share, publish, save or replicate it in any way
- The DPO will ensure a written response is received from the individual who received the correspondence, confirming that they have complied with the request to return the correspondence and not to share, publish, save or replicate it in any way

Appendix 2: Privacy Notice - Students

Privacy Notice (How we use student information)

Under UK data protection law, individuals have a right to be informed about how Prince Henry's High School (Prince Henry's/the school) uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about students at the school.

Prince Henry's High School, Victoria Avenue, Evesham WR11 4QH, is the 'data controller' for the purposes of UK data protection law.

Our Data Protection Officer is Mrs M Wall (see 'Contact' below).

The categories of student information that we process include:

- Personal identifiers and contacts (such as name, unique student number, contact details and address)
- Characteristics (such as ethnicity, language, and free school meal eligibility)
- Safeguarding information (such as court orders and professional involvement)
- Special educational needs (including the needs and ranking)
- Medical and administration (such as doctors' information; child health, including physical and mental health; dental health; allergies; medication and dietary requirements)
- Attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Assessment and attainment (such as internal and external examination results, post 16 courses enrolled for)
- Behavioural information (such as suspensions and any relevant alternative provision put in place)
- Where students go after they leave Prince Henry's High School
- Photographs, videos and CCTV images captured in school in accordance with our Data Protection Policy
- Biometric information in accordance with our Data Protection Policy
- Trips and activities
- Catering and free school meal management
- Identity management/authentication

The school may also hold student data that has been received from other organisations, including other schools and social services.

This list is not exhaustive, to access the current list of categories of information we process please contact the school's Data Protection Officer.

Why we collect and use student information

We collect and use student information, for the following purposes:

- a. To support student learning
- b. To monitor and report on student attainment progress
- c. To provide appropriate pastoral care
- d. To protect student welfare
- e. To assess the quality of our services
- f. To administer admissions waiting lists
- g. To keep children safe (food allergies, or emergency contact details)
- h. To meet the statutory duties placed upon us for DfE data collections
- i. To support a young person in their transition to a post-16 Provider of Education or Training

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing student information are:

- To collect the information, or the information is necessary for us to meet legal requirements, such as our duty to safeguard students. (Article 6, 1c UK GDPR)
- To hold and use information for the purposes of providing schooling and so we can look after our students. (Article 6, 1e UK GDPR)
- Explicit permission is sometimes required to use student information. This includes taking pictures or videos of students to be used on our website or in the newspaper. Prior consent will be sought from either parents/carers or students directly. (Article 6, 1a UK GDPR). Consent may be withdrawn at any time by contacting secretary@princehenrys.worcs.sch.uk.

In addition, concerning any special category data: the school will only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your child's personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your child's life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it 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
- We need to process it 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

- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your child's life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

All of the special category personal data above is covered in Article 9, sections 2a, 2c, 2f, 2g and 2i of the UK GDPR.

Compliance with all of the above enables the school to meet its obligations:

- To allow the school to effectively carry out its duties under the Education Act 1996. In particular the requirement under section 537a of the Education Act 1996 to provide individual pupil information to the Department of Education as required.
- To ensure the wellbeing and safety of pupils in line with keeping Children Safe in Education statutory guidance with reference to Section 175 of the Education Act 2002.
- School Attendance and Parental Responsibility Measures statutory guidance
- Education and Inspections Act 2006, The children's Act 2004 (section 12, 14B, 54)
- SEND code of practice relating to part 3 of the Children and Families Act 2014
- Supporting pupils with medical conditions at school guidance relating to section 100 of the Children and Families Act 2014

Collecting student information

We collect student information primarily via admission and registration forms completed by parents/carers and Common Transfer File (CTF) or secure file transfer from the previous school. We may also hold data that has been provided by:

- Local Authorities
- Government departments or agencies
- Police forces, courts, tribunals

Student data is essential for the schools' operational use. Whilst the majority of student information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain student information to us or if you have a choice in this.

Storing student data

We hold student data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please see the school's Data Protection Policy, which is available on the school's website:

<https://www.princehenrys.worcs.sch.uk/policies-statutory-information/>

Who we share student information with

We routinely share student information with:

- Schools that the students attend after leaving us
- Our local authority
- Non-local authority professionals and agencies with whom we have a duty to co-operate (eg NHS)
- Youth support services (students aged 13+)
- The Department for Education (DfE)
- Education and homework software systems. These systems relate to our public task to provide students with an education.

Why we regularly share student information

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with UK data protection law), we may share personal information about students with:

- Our regulator, Ofsted
- Suppliers and service providers:
 - Catering providers (biometric/allergy/cashless data)
 - Educational software providers
- Financial organisations
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals

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

The information shared is limited to the child's name, address and date of birth. However where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / student once they reach the age 16.

Data is securely transferred to the youth support service via the local authority's secure data portal.

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 13-19 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

Data is securely transferred to the youth support service via the local authority's secure data portal.

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

Department for Education (DfE)

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

All data is transferred securely and held by the Department for Education (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, 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, contact school's Data Protection Officer, Mrs M Wall (contact details below).

You also have the right to:

- To ask us for access to information about you that we hold
- To have your personal data rectified, if it is inaccurate or incomplete
- To request the deletion or removal of personal data where there is no compelling reason for its continued processing
- To restrict our processing of your personal data (i.e. Permitting its storage but no further processing)
- To object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- Not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you

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

For further information on how to request access to personal information held centrally by the Department for Education (DfE), please see the 'How 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 school's Data Protection Officer, Mrs M Wall (contact details below).

Last updated

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated on 1st September 2023.

Contact

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

Mrs M Wall Data Protection Officer
 Prince Henry's High School
 Victoria Avenue
 Evesham
 WR11 4QH
 Tel: 01386 765588
 Email: secretary@princehenrys.worcs.sch.uk

Appendix 3 UK GDPR: Retention and Disposal of Records

Prince Henry's High School follows the procedures set out in the table below in relation to the retention and disposal of data securely. This is in line with the current guidance as one of the 7 principles of the UK GDPR Regulations.

Document Type	Retention Period	Action at end of retention period
Secondary School Student Records	Until the students 25 birthday	Dispose of records securely. If the student leaves to another educational setting, transfer the records to the new school
Special Education Needs and Disabilities	6 years from the end of the EHCP	Dispose of records securely. If the student leaves to another educational setting, transfer the records to the new school
Child Protection Files	Until the child's 25 birthday	Child protection files should be passed on If the student leaves to another educational setting, transfer the records to the new school - separately from the main school file.
Child Sexual Abuse	75 years	Child protection files should be passed on If the student leaves to another educational setting, transfer the records to the new school - separately from the main school file.
Allegations of Child Protection Against a Member of Staff Including unfounded later.	Until the staff members normal retirement age, or 10 years from the date of the allegation, whichever is later	Dispose of records securely