
DATA PROTECTION AND GDPR

PREFACE

Chiltern Hills Academy is a learning environment at the heart of its community. We encourage every person in our community to:

Create, Aspire and Excel to ‘Live life in all its fullness’ (John 10:10)

We achieve this through our dedication to the seven Christian values of love, hope, self-discipline, compassion, forgiveness, respect and honesty.

We are a community in which staff, students and parents work collaboratively to develop a learning environment and organisation which is spiritual, safe, innovative, creative and exciting. All members of the Academy are motivated and inspired by the vision to give their best and to play a full part in the life of the school and in their own developing lives.

The Governors at Chiltern Hills Academy are committed to achieving the vision and values. They oversee and monitor this policy to ensure that this is being achieved.

Contents

1. Aims	3
2. Legislation & Guidance	3
3. Definitions.....	3
4. The Data Controller	4
5. Roles & Responsibilities	5
6. Data Protection Principles.....	6
7. Collecting Personal Data	6
8. Sharing Personal Data.....	8
9. Subject Access Requests and other Rights of Individuals	9
10. Parental requests to see Educational Record	11
11. Biometric Recognition Systems	11
12. CCTV.....	12
13. Photographs & Videos	12
14. Data Protection by Design & Default.....	13
15. Data Security & Storage of Records	13
16. Disposal of Records.....	14
17. Personal Data Breaches	14
18. Training	14
19. Monitoring Arrangements.....	15
20. Links with Other Policies.....	15

DATA PROTECTION AND GDPR

Appendix 1 – Personal Data Breach Procedure..... 15
Appendix 2 – Privacy Notices 19

DATA PROTECTION AND GDPR

1. Aims

We (Chiltern Hills Academy) aim to ensure that all personal data collected about staff, students, parents, governors, volunteers, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

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

2. Legislation & Guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

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

3. Definitions

Term	Definition
Personal Data	<p>Any information relating to an identified, or identifiable, living individual. This may include the individual's:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>

DATA PROTECTION AND GDPR

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: <ul style="list-style-type: none">• Racial or ethnic origin• Political opinions• Religious or philosophical beliefs• Trade union membership• Genetics• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes• Health – physical or mental• Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

Our Academy processes personal data relating to parents, students, staff, governors, visitors, volunteers and other individuals, and therefore is a data controller.

DATA PROTECTION AND GDPR

The Academy is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

5. Roles & Responsibilities

This policy applies to all staff, students, parents, governors, volunteers, visitors and other individuals at Chiltern Hills Academy, and to external organisations or individuals working on our behalf. Staff, students, parents, governors, volunteers, visitors and other individuals who do not comply with this policy may face disciplinary or legal action.

Governing Board

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

Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with Data Protection Law, and developing related policies and guidelines where applicable.

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

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

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

Our DPO's contact details are below:

Data Protection Officer
Kathy Buxton
Chiltern Hills Academy
Chartridge Lane
Chesham
Buckinghamshire
HP5 2RG
Email: dataprotection@chacademy.co.uk
Telephone: 01494 782066

Principal

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

DATA PROTECTION AND GDPR

All staff, students, parents, governors, volunteers, visitors and other individuals

are responsible for:

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

6. Data Protection Principles

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

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

7. Collecting Personal Data

a. Lawfulness, fairness and transparency

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

- The data needs to be processed so that the Academy can fulfil a contract with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person e.g. to protect someone's life

DATA PROTECTION AND GDPR

- The data needs to be processed so that the Academy, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the Academy (where the processing is not for any tasks the Academy performs as a public authority) 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 under data protection law:

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

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

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

DATA PROTECTION AND GDPR

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

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

b. Limitation, minimisation and accuracy

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

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

Staff, students, parents, governors, volunteers, visitors and other individuals must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

When staff, students, parents, governors, volunteers, visitors and other individuals no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

8. Sharing Personal Data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with the Academy that puts the safety of our staff, students, parents, governors, volunteers, visitors and other individuals at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff, students, parents, governors, volunteers, visitors and other individuals – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we

are legally required to do so.

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 staff, students, parents, governors, volunteers, visitors and other individuals.

Where we transfer personal data internationally we will do so in accordance with data protection law.

9. Subject Access Requests and other Rights of Individuals

a. Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing to the DPO and include:

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

If staff, students, parents, governors, volunteers, visitors and other individuals receive a subject access request they must immediately forward it to the DPO.

b. Children and subject access requests

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

Children below the age of 12:

DATA PROTECTION AND GDPR

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our Academy may 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.

Children aged 12 and above:

Children aged 12 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 our Academy 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.

c. Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

d. Other data protection rights of the individual

DATA PROTECTION AND GDPR

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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, students, parents, governors, volunteers, visitors and other individuals receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see Educational Record

A request for a student's Educational Record should be made directly to the Principal. Any request for a student's Educational Records received by staff, students, parents, governors, volunteers, visitors and other individuals must be immediately forwarded to the Principal.

11. Biometric Recognition Systems

Where the Academy uses students' biometric data as part of an automated biometric recognition system (for example, students use biometric data for catering services), 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. The Academy 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 the Academy's biometric system. We will provide alternative means of accessing the relevant services for those students.

Parents/carers and students can 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).

DATA PROTECTION AND GDPR

Where staff members or other adults use the Academy's biometric system, 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 the Academy will delete any relevant data already captured.

12. CCTV

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

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

Any enquiries about the CCTV system should be directed to the Data Protection Officer (DPO).

13. Photographs & Videos

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

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

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. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

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

Where the Academy takes photographs and videos, uses may include:

- Within the Academy on notice boards and in Academy magazines, brochures, newsletters, etc.
- Outside the Academy by external agencies such as the Academy photographer, newspapers, campaigns
- Online on our Academy website or social media pages
- Lessons which are recorded on MS Teams

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

When using photographs and videos in this way we will not accompany them with any

DATA PROTECTION AND GDPR

other personal information about the student, to ensure they cannot be identified.

Please see additional information and conditions of use, stated at the time of giving consent, for more information on our use of photographs and videos.

Where lessons are recorded on MS Teams, these will be retained for a period of two years in order that they may be used as a medium term resource.

14. Data Protection by Design & Default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the Academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our Academy and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

15. Data Security & Storage of Records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

DATA PROTECTION AND GDPR

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Passwords that are at least 10 characters long containing letters and numbers are used by staff to access Academy computers, laptops and other electronic devices. Staff and students are reminded that they should not reuse passwords from other sites.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices where personal information is stored
- Staff, students, parents, governors, volunteers, visitors and other individuals who store personal information on their personal devices are expected to follow the same security procedures as for Academy-owned equipment (see our E-Safety policy on acceptable use)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of Records

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

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Academy'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

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

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

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

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

18. Training

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

DATA PROTECTION AND GDPR

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

19. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every 2 years** and shared with the full governing board.

20. Links with Other Policies

This data protection policy is linked to other policies including:

- Freedom of information policy

MONITORING, EVALUATION AND REVIEW

This policy will be reviewed at least every two years, or when there are changes in the law to assess implementation and effectiveness. This policy will be promoted and implemented throughout the Academy.

DATA PROTECTION AND GDPR

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

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

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the DPO on the Trust's central systems.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 1231113), within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned

DATA PROTECTION AND GDPR

- The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
 - The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - A description, in clear and plain language, of the nature of the personal data breach
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

As above, any decision on whether to contact individuals will be documented by the DPO.

- 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 by the DPO on the Trust's central systems.

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

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff, students, parents, governors, volunteers, visitors and other individuals who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it

DATA PROTECTION AND GDPR

- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach could include:

- Details of pupil premium interventions for named children being published on the Academy website
- Non-anonymised student exam results or staff pay information being shared with governors
- An Academy laptop containing non-encrypted sensitive personal data being stolen or hacked
- The Academy's cashless payment provider being hacked and parents' financial details stolen

Appendix 2 – Privacy Notices

2.1 Privacy Notice for Staff/Volunteers

Under data protection law, individuals have a right to be informed how Chiltern Hills Academy uses any personal data that we hold about them. We comply with this right by providing privacy notices to individuals where we are processing their personal data.

This privacy notice explains how we collect, use, store and share personal data about individuals we employ, or otherwise engage to work at our Academy, and individuals working with our Academy in a voluntary capacity.

We (Chiltern Hills Academy) aim to ensure that all personal data is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

We (Chiltern Hills Academy) are a data controller for the purposes of Data Protection Law.

Contact details for our Data Protection Officer are listed below (see 'Contact').

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth
- Next of kin and emergency contact numbers
- Salary, annual leave, pension
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence and vehicle details
- Information about business and pecuniary interests
- Data about your use of the Academy's information and communications system

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about gender, ethnicity, religious beliefs
- Photographs and CCTV images captured in the Academy
- Information about any health conditions you have that we need to be aware of and sickness records

DATA PROTECTION AND GDPR

- Information about disability and any access requirements
- Biometric data

We may also collect, use, store and share (where appropriate) information about criminal convictions and offences.

We may also use, store and share data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

Why we use this data

The purpose of processing this data is to support the Academy to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards students
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable equalities monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body
- Ensure that appropriate access arrangements can be provided for individuals who require them

Use of your personal data in automated decision making and profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Our lawful basis for using this data

Our lawful bases for processing your personal data for the purposes listed above are in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR).

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

- The data needs to be processed so that the Academy can fulfil a contract with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person e.g. to protect someone's life

DATA PROTECTION AND GDPR

- The data needs to be processed so that the Academy, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the Academy (where the processing is not for any tasks the Academy performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual has freely given clear consent

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data

For 'special category' data, we only collect and use it where we have both a lawful basis, as set out above, and one of the following conditions as set out in data protection law:

- We have obtained your explicit consent to use your 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 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 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 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

DATA PROTECTION AND GDPR

Collecting this data

While the majority of information we collect from you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from local authorities, government departments or agencies, police forces, courts or tribunals.

How we store this data

Personal data is stored in accordance with our Data Protection Policy.

We create and maintain electronic records and an employment file for individuals we employ, or otherwise engage to work at our Academy, and individuals working with our Academy in a voluntary capacity. The information is kept secure and is only used for purposes directly relevant to your employment.

We will retain and dispose of your personal information in accordance with the Information and Records Management Society's toolkit for schools.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

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

- The Academy sponsors (Diocese of Oxford, Buckinghamshire Council)
- Local Authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Government department or agencies
- Your family or representatives
- Educators and examining bodies
- Our regulators
- Non-Academy employees such as Governors, referees
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll, catering
- Our auditors

DATA PROTECTION AND GDPR

- Financial organisations
- Health authorities and health and social organisations
- Professional advisers and consultants
- Security organisations
- Police forces, courts, tribunals

Transferring data internationally

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.

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Use of your personal information for communication purposes

As per our lawful basis for using data, the Academy may send you communication and information about Chiltern Hills Academy or PTA or local or related activities, events, campaigns, charitable causes or services.

Your rights

a. How to access personal information we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy holds about them.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our Data Protection Officer.

b. Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

DATA PROTECTION AND GDPR

- Object to the use of your personal data
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, have personal data we hold about you deleted or destroyed, or restrict processing
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Data Protection Officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

Data Protection Officer
Kathy Buxton
Chiltern Hills Academy
Chartridge Lane
Chesham
Buckinghamshire
HP5 2RG
Email: dataprotection@chacademy.co.uk
Telephone: 01494 782066

This notice is based on the Department for Education's model Privacy Notice for the school workforce and The Key for School Leaders model Privacy Notice for the school workforce amended to reflect the way we use data in Chiltern Hills Academy.

2.2 Privacy Notice for Governors/Trustees

Under data protection law, individuals have a right to be informed how Chiltern Hills Academy uses any personal data that we hold about them. We comply with this right by providing privacy notices to individuals where we are processing their personal data.

This privacy notice explains how we collect, use, store and share personal data about individuals working with our Academy in a voluntary capacity, including governors/trustees.

We (Chiltern Hills Academy) aim to ensure that all personal data is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

We (Chiltern Hills Academy) are a data controller for the purposes of Data Protection Law.

Contact details for our Data Protection Officer are listed below (see 'Contact').

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Name and contact details
- References
- Evidence of qualifications
- Employment details
- Information about business and pecuniary interests

We may also collect, use, store and share information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to, information about:

- Information about disability and any access requirements
- Information about any health conditions that we need to be aware of
- Religious beliefs (for Oxford Diocese Governors)
- Photographs and CCTV images captured in the Academy

We may also collect, use, store and share (where appropriate) information about criminal convictions and offences.

We may also use, store and share data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

Why we use this data

The purpose of processing this data is to support the Academy to:

- Establish and maintain effective governance

DATA PROTECTION AND GDPR

- Meet statutory obligations for publishing and sharing governors'/trustees' details
- Facilitate safe recruitment, as part of our safeguarding obligations towards students
- Ensure that appropriate access arrangements can be provided for individuals who require them

Use of your personal data in automated decision making and profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Our lawful basis for using this data

Our lawful bases for processing your personal data for the purposes listed above are in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR).

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

- The data needs to be processed so that the Academy can fulfil a contract with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person e.g. to protect someone's life
- The data needs to be processed so that the Academy, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the Academy (where the processing is not for any tasks the Academy performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual has freely given clear consent

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data

For 'special category' data, we only collect and use it where we have both a lawful basis, as set out above, and one of the following conditions as set out in data protection law:

- We have obtained your explicit consent to use your 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 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

DATA PROTECTION AND GDPR

- 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 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 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

Collecting this data

While the majority of information we collect from you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from local authorities, government departments or agencies, police forces, courts or tribunals.

How we store this data

Personal data is stored in accordance with our Data Protection Policy.

We keep personal information about you while you volunteer our Academy. We may also keep it beyond your work with our Academy if this is necessary. We create and maintain electronic records and files for individuals volunteering at our Academy. The information is kept secure and is only used for purposes directly relevant to your role with the Academy.

We will retain and dispose of your personal information in accordance with the Information and Records Management Society's toolkit for schools.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

DATA PROTECTION AND GDPR

We will dispose of your personal data securely when we no longer need it.

Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

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

- The Academy sponsors (Diocese of Oxford, Buckinghamshire County Council)
- Government departments or agencies
- Local Authority – to meet our legal obligations to share certain information such as safeguarding concerns
- Our regulators [Ofsted, SIAMS]
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Our auditors
- Financial organisations
- Professional advisors and consultants
- Health and social welfare organisations
- Police forces, courts, tribunals

Transferring data internationally

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.

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

a. How to access personal information we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

DATA PROTECTION AND GDPR

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our Data Protection Officer.

b. Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, have the personal data we hold about you deleted or destroyed, or restrict processing
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Data Protection Officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

Data Protection Officer
Kathy Buxton
Chiltern Hills Academy
Chartridge Lane

DATA PROTECTION AND GDPR

Chesham
Buckinghamshire
HP5 2RG
Email: dataprotection@chacademy.co.uk
Telephone: 01494 782066

This notice is based on the Department for Education's model Privacy Notice for the school workforce and The Key for School Leaders model Privacy Notice for governors/trustees and other volunteers, amended to reflect the way we use data in Chiltern Hills Academy.

2.3 Privacy Notice for Parents/Carers – use of your personal data

Under data protection law, individuals have a right to be informed how Chiltern Hills Academy uses any personal data that we hold about them. We comply with this right by providing privacy notices to individuals where we are processing their personal data.

This privacy notice explains how we collect, use, store and share personal data about parents/carers of students at our Academy.

We (Chiltern Hills Academy) aim to ensure that all personal data is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

We (Chiltern Hills Academy) are a data controller for the purposes of Data Protection Law. Contact details for our Data Protection Officer are listed below (see 'Contact').

The personal data we hold

Personal data that we may collect, use, store and share (where appropriate) includes, but is not restricted to:

- Contact details and contact preferences such as your name, address, email address and telephone numbers
- Details of your family circumstances
- Records of your correspondence and contact with us
- Details of any complaints you have made

We may also collect, use, store and share (where appropriate) information that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to information about:

- Any health conditions you have that we need to be aware of
- Gender and relationship to child
- Details of any safe guarding information including court orders or professional involvement
- Photographs and CCTV images captured in the Academy
- Information about any access requirements

We may also use, store and share data about you that we have received from other organisations, including other schools and social services.

Why we use this data

The information is collected and used because it is required by our Academy in order to carry out the task of educating and ensuring the welfare of our students.

The purpose of processing this data is to support the Academy to:

- Report to you on your child's attainment and progress

DATA PROTECTION AND GDPR

- Keep you informed about the running of the Academy (such as emergency closures) and events
- Process payments for Academy services
- To provide appropriate pastoral care
- To assess the quality of our services
- To protect student welfare
- To administer admissions waiting lists
- Carry out research
- To comply with our legal and statutory obligations
- Ensure that appropriate access arrangements can be provided for individuals who require them

We also collect and use parent/carer information in order to help students with additional special needs and requirements, so that we can ensure we offer the best possible support and resources to them and their parents and carers during their time in our Academy.

We may also process parent/carer's personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Use of your personal data in automated decision making and profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Our lawful basis for using this data

Our lawful bases for processing personal data for the purposes listed above are in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR).

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

- The data needs to be processed so that the Academy can fulfil a contract with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person e.g. to protect someone's life
- The data needs to be processed so that the Academy, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the Academy (where the processing is not for any tasks the Academy performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual has freely given clear consent

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would

DATA PROTECTION AND GDPR

go about withdrawing consent if you wish to do so.

Our basis for using special category data

For 'special category' data, we only collect and use it where we have both a lawful basis, as set out above, and one of the following conditions as set out in data protection law:

- We have obtained your explicit consent to use your 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 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 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 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

Collecting this data

While the majority of information we collect from you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from local authorities, government departments or agencies, police forces, courts or tribunals.

DATA PROTECTION AND GDPR

How we store this data

Personal data is stored in accordance with our Data Protection Policy.

We keep personal information about you while your child is attending our Academy. We may also keep it beyond their attendance at our Academy if this is necessary. The information is kept secure and is only used for purposes directly relevant to your child attending the Academy.

We hold student data up until their 25th birthday.

We hold student data for Special Educational Needs students up until their 30th birthday.

We may hold information about parents/carers along with student records until this date.

We will retain and dispose of your personal information in accordance with the Information and Records Management Society's toolkit for schools.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Who do we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

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

- Schools that the student attends after leaving us
- The local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about exclusions
- Government departments or agencies such as the Department for Education (DfE)
- Our regulators (Ofsted, SIAMS)
- Non-Academy employees such as Governors
- Suppliers and service providers, professional advisors and consultants – to enable them to provide the service we have contracted them for such as Caterlink
- Our auditors
- NHS, health and social welfare organisations and authorities
- Charities and voluntary organisations such as Duke of Edinburgh's Award
- Police forces, courts and tribunals

Transferring data internationally

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

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

DATA PROTECTION AND GDPR

Your rights

a. How to access personal information that we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy holds about them.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our Data Protection Officer.

b. Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, have personal data we hold about you deleted or destroyed, or restrict processing
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

DATA PROTECTION AND GDPR

To make a complaint, please contact our Data Protection Officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

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

Kathy Buxton
(Data Protection Officer)
Chiltern Hills Academy
Chartridge Lane
Chesham
Buckinghamshire
HP5 2RG

Email: dataprotection@chacademy.co.uk
Telephone: 01494 782066

This Privacy Notice is based on the model Privacy Notice of Oxford Diocesan Schools Trust and The Key for School Leaders model Privacy Policy for parents and carers – use of your personal data, and amended to reflect the way that we use data in Chiltern Hills Academy.

2.4 Privacy Notice for Parents/Carers – use of your child’s personal data

Under data protection law, individuals have a right to be informed how Chiltern Hills Academy uses any personal data that we hold about them. We comply with this right by providing privacy notices to individuals where we are processing their personal data.

This privacy notice explains how we collect, use, store and share personal data about students at our Academy.

We (Chiltern Hills Academy) aim to ensure that all personal data is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

We (Chiltern Hills Academy) are a data controller for the purposes of Data Protection Law. Contact details for our Data Protection Officer are listed below (see ‘Contact’).

The personal data we hold

Personal data that we may collect, use, store and share (where appropriate) includes, but is not restricted to:

- Personal information such as name, date of birth, identification documents, unique pupil number and address
- Attendance information such as sessions attended, number of absences and absence reasons
- Student and curricular records
- Details of any siblings who attend/have attended Chiltern Hills Academy
- Results of internal assessment and externally set tests
- Exclusions/behavioural information
- Post-16 learning information

We may also collect, use, store and share (where appropriate) information that falls into ‘special categories’ of more sensitive personal data. This includes, but is not restricted to:

- Relevant medical information including physical and mental health
- Information about gender, ethnicity, religious beliefs, language
- Details of any support received, including care packages, plans and support providers
- Free school meal eligibility
- Special educational needs information
- Safeguarding information
- Biometric information for catering services
- Photographs and CCTV images captured in the Academy
- Passport details if applicable

We may also use, store and share data about our students that we have received from other organisations, including other schools and social services.

DATA PROTECTION AND GDPR

Why we use this data

The information is collected and used because it is required by our Academy in order to carry out the task of educating and ensuring the welfare of our students.

The purpose of processing this data is to support the Academy to:

- To support student teaching and learning
- To monitor and report on student progress
- To provide appropriate pastoral care
- To assess the quality of our services
- To protect student welfare
- To administer admissions waiting lists
- Carry out research
- To comply with the law regarding data sharing
- Ensure that appropriate access arrangements can be provided for individuals who require them

We also collect and use student information in order to help students with additional special needs and requirements, so that we can ensure we offer the best possible support and resources to them (and their parents and carers) during their time in our Academy.

We may also process student's personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests).

Use of student personal data in automated decision making and profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Our lawful basis for using this data

Our lawful bases for processing our student's personal data for the purposes listed above are in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR).

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

- The data needs to be processed so that the Academy can fulfil a contract with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person e.g. to protect someone's life
- The data needs to be processed so that the Academy, as a public authority, can perform a task in the public interest or exercise its official authority

DATA PROTECTION AND GDPR

- The data needs to be processed for the legitimate interests of the Academy (where the processing is not for any tasks the Academy performs as a public authority) 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

Where you have provided us with consent to use your child's data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data

For 'special category' data, we only collect and use it where we have both a lawful basis, as set out above, and one of the following conditions as set out in 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 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

Collecting this data

We collect student information via admission forms and information provided from you, Common Transfer Files (CTF) or secure file transfer from another school.

DATA PROTECTION AND GDPR

Whilst the majority of student information you provide to us is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about your child will come from you, but we may also hold data from local authorities, government departments or agencies, police forces, courts or tribunals.

How we store this data

Personal data is stored in accordance with our Data Protection Policy.

We keep personal information about your child while they are attending our Academy. We may also keep it beyond their attendance at our Academy if this is necessary. The information is kept secure and is only used for purposes directly relevant to your child attending the Academy.

We hold student data up until their 25th birthday.

We hold student data for Special Educational Needs students up until their 30th birthday.

We will retain and dispose of your personal information in accordance with the Information and Records Management Society's toolkit for schools.

We have put in place appropriate security measures to prevent your child's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your child's personal data securely when we no longer need it.

Who we share data with

We do not share information about your child with any third party without consent unless the law and our policies allow us to do so.

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

- Schools that the student attends after leaving us
- The local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about exclusions
- Government departments or agencies such as the Department for Education (DfE)
- Educators and examining bodies
- The student's family and representatives
- Our regulators (Ofsted, SIAMS)
- Non-Academy employees such as Governors
- Suppliers and service providers, professional advisors and consultants – to enable them to provide the service we have contracted them for such as Caterlink
- Our auditors
- NHS, health and social welfare organisations and authorities

DATA PROTECTION AND GDPR

- Charities and voluntary organisations such as Duke of Edinburgh's Award
- Police forces, courts and tribunals

Transferring data internationally

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

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Aged 14+ qualifications

For students enrolling for post 14 qualifications, the Learning Records Service will give us a student's unique learner number (ULN) and may also give us details about the student's learning or qualifications.

Why we 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.

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our students with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements

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

Youth support services

What is different about students aged 13+?

Once our students reach the age of 13, we also pass student and parent/carer 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

DATA PROTECTION AND GDPR

A parent/carer can request that only their and their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child/student once he/she reaches the age 16.

Our 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

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

The National Pupil 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.

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

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

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

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

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance

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

DATA PROTECTION AND GDPR

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

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

For more information about the department's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided student information, (and for which project), please visit the following website:

<https://www.gov.uk/government/publications/national-pupil-database-requests-received>

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

Your rights

a. How to access personal information that we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy holds about them.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our Data Protection Officer.

b. Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data
- Prevent your data being used to send direct marketing

DATA PROTECTION AND GDPR

- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, have personal data we hold about you deleted or destroyed, or restrict processing
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Data Protection Officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

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

Kathy Buxton
(Data Protection Officer)
Chiltern Hills Academy
Chartridge Lane
Chesham
Buckinghamshire
HP5 2RG

Email: dataprotection@chacademy.co.uk
Telephone: 01494 782066

This Privacy Notice is based on the model Privacy Notice of Oxford Diocesan Schools Trust and The Key for School Leaders model Privacy Notice for parents and carers – use of your child's personal data, and amended to reflect the way that we use data in Chiltern Hills Academy.

2.5 Privacy Notice for Visitors and Hirers

Under data protection law, individuals have a right to be informed how Chiltern Hills Academy uses any personal data that we hold about them. We comply with this right by providing privacy notices to individuals where we are processing their personal data.

This privacy notice explains how we collect, use, store and share personal data about visitors to the Academy and hirers of the Academy.

We (Chiltern Hills Academy) aim to ensure that all personal data is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

We (Chiltern Hills Academy) are a data controller for the purposes of Data Protection Law.

Contact details for our Data Protection Officer are listed below (see 'Contact').

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Name and contact details
- Information relating to the visit or hire such as company or organisation name, arrival and departure time, vehicle details
- Bank account details (if applicable)
- Insurance details (if applicable)

We may also collect, store and use information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to, information about:

- Information about any access requirements
- Photographs and CCTV images captured in the Academy

We may also use, store and share data about you that we have received from other organisations, including other schools and social services.

Why we use this data

The purpose of processing this data is to support the Academy to:

- Identify you and keep you safe while on the Academy site
- Keep students, staff and visitors safe while you are on the Academy site
- Maintain accurate records of visits to the school
- Ensure that appropriate access arrangements can be provided for individuals who require them
- To enable the Academy to hire facilities to you

DATA PROTECTION AND GDPR

Use of your personal data in automated decision making and profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Our lawful basis for using this data

Our lawful bases for processing your personal data for the purposes listed above are in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR).

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

- The data needs to be processed so that the Academy can fulfil a contract with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person e.g. to protect someone's life
- The data needs to be processed so that the Academy, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the Academy (where the processing is not for any tasks the Academy performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual has freely given clear consent

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data

For 'special category' data, we only collect and use it where we have both a lawful basis, as set out above, and one of the following conditions as set out in data protection law:

- We have obtained your explicit consent to use your 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 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

DATA PROTECTION AND GDPR

- 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 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 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

Collecting this data

While the majority of information we collect from you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from local authorities, government departments or agencies, police forces, courts or tribunals.

How we store this data

Personal data is stored in accordance with our Data Protection Policy.

We keep personal information about you while you are visiting our Academy. We may also keep it beyond your visit if this is necessary. We create and maintain electronic records and files for individuals hiring our Academy. The information is kept secure and is only used for purposes directly relevant to your hire of the Academy.

We will retain and dispose of your personal information in accordance with the Information and Records Management Society's toolkit for schools.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

DATA PROTECTION AND GDPR

Data sharing

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

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

- The Academy sponsors (Diocese of Oxford, Buckinghamshire County Council)
- Government departments or agencies
- Local Authority – to meet our legal obligations to share certain information such as safeguarding concerns
- Our regulators [Ofsted, SIAMS]
- Non-Academy employees such as Governors
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as BookingsPlus
- Our auditors
- Financial organisations
- Professional advisors and consultants
- Health and social welfare organisations
- Police forces, courts, tribunals

Transferring data internationally

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.

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

a. How to access personal information we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

DATA PROTECTION AND GDPR

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our Data Protection Officer.

b. Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, have the personal data we hold about you deleted or destroyed, or restrict processing
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Data Protection Officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

DATA PROTECTION AND GDPR

Data Protection Officer
Kathy Buxton
Chiltern Hills Academy
Chartridge Lane
Chesham
Buckinghamshire
HP5 2RG
Email: dataprotection@chacademy.co.uk
Telephone: 01494 782066

This notice is based on the The Key for School Leaders model Privacy Notice for visitors, amended to reflect the way we use data in Chiltern Hills Academy.

2.6 Privacy Notice for Job Applicants

Under data protection law, individuals have a right to be informed how Chiltern Hills Academy uses any personal data that we hold about them. We comply with this right by providing privacy notices to individuals where we are processing their personal data.

This privacy notice explains how we collect, use, store and share personal data about individuals applying for jobs at our Academy.

We (Chiltern Hills Academy) aim to ensure that all personal data is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

We (Chiltern Hills Academy) are a data controller for the purposes of Data Protection Law.

Contact details for our Data Protection Officer are listed below (see 'Contact').

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Name and contact details
- Copies of right to work documentation
- References
- Evidence of qualifications
- Employment records, including work history, job titles, training records and professional memberships
- Other information included in a CV or cover letter as part of the application process

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to, information about:

- Information about gender, ethnicity, religious beliefs
- Information about disability and access arrangements
- Photographs and CCTV images captured in school

We may also collect, use, store and share (where appropriate) information about criminal convictions and offences.

We may also use, store and share data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

Why we use this data

The purpose of processing this data is to support the Academy to:

DATA PROTECTION AND GDPR

- Enable us to establish relevant experience and qualifications
- Facilitate safe recruitment, as part of our safeguarding obligations towards students
- Enable equalities monitoring
- Ensure that appropriate access arrangements can be provided for individuals that require them

Use of your personal data in automated decision making and profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Our lawful basis for using this data

Our lawful bases for processing your personal data for the purposes listed above are in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR).

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

- The data needs to be processed so that the Academy can fulfil a contract with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person e.g. to protect someone's life
- The data needs to be processed so that the Academy, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the Academy (where the processing is not for any tasks the Academy performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual has freely given clear consent

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data

For 'special category' data, we only collect and use it where we have both a lawful basis, as set out above, and one of the following conditions as set out in data protection law:

- We have obtained your explicit consent to use your 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 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

DATA PROTECTION AND GDPR

- 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 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 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

Collecting this data

While the majority of information we collect from you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from local authorities, government departments or agencies, police forces, courts or tribunals.

How we store this data

Personal data is stored in accordance with our Data Protection Policy.

We keep personal information about you during the application process. We may also keep it beyond this if this is necessary. The information is kept secure and is only used for purposes directly relevant to the application process.

We will retain and dispose of your personal information in accordance with the Information and Records Management Society's toolkit for schools.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

DATA PROTECTION AND GDPR

We will dispose of your personal data securely when we no longer need it.

Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

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

- The Academy sponsors (Diocese of Oxford, Buckinghamshire County Council)
- Government departments or agencies
- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Non-Academy employees such as Governors, referees
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Professional advisers and consultants
- Employment and recruitment agencies
- Police forces, courts and tribunals

Transferring data internationally

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.

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

a. How to access personal information we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy holds about them.

If you make a subject access request, and if we do hold information about you, we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

DATA PROTECTION AND GDPR

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our Data Protection Officer.

b. Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, have personal data we hold about you deleted or destroyed, or restrict processing
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Data Protection Officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

Data Protection Officer
Kathy Buxton
Chiltern Hills Academy
Chartridge Lane

DATA PROTECTION AND GDPR

Chesham
Buckinghamshire
HP5 2RG
Email: dataprotection@chacademy.co.uk
Telephone: 01494 782066

This notice is based on The Key for School Leaders model Privacy Notice for job applicants amended to reflect the way we use data in Chiltern Hills Academy.

2.7 Privacy Notice for Suppliers of Goods and Services

Under data protection law, individuals have a right to be informed how Chiltern Hills Academy uses any personal data that we hold about them. We comply with this right by providing privacy notices to individuals where we are processing their personal data.

This privacy notice explains how we collect, use, store and share personal data about suppliers of goods and services that the Academy contracts with, including their individual representatives, employees and agents. References to 'you' in this privacy notice cover all of these individuals.

We (Chiltern Hills Academy) aim to ensure that all personal data is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

We (Chiltern Hills Academy) are a data controller for the purposes of Data Protection Law.

Contact details for our Data Protection Officer are listed below (see 'Contact').

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Names, characteristics and contact details
- References, CVs and details of an individual's employment history, if collected as part of a bidding, tendering or engagement process
- Bank details and other financial information where it relates to an individual such as if you're operating as a sole trader
- Any other personal information necessary to fulfil the terms of a contract we have with you
- Information relating to visits to the school such as the individual's company or organisation name, arrival and departure time, vehicle details

If our contract with you requires you to visit or carry out any work at the school site, our privacy notice for visitors to the school will also apply.

We may also collect, store and use information about you that falls into 'special categories' of more sensitive personal data. This includes but is not restricted to:

- Information about any access arrangements
- Photographs for identification purposes
- CCTV images captured in school

We may also use, store and share data about you that we have received from other organisations, including other schools and social services.

DATA PROTECTION AND GDPR

Why we use this data

The purpose of processing this data is to support the Academy to:

- Decide whether to engage you
- Fulfil the terms of our contract with you, including payment
- Keep accurate records of the suppliers we use
- Identify you while on the Academy site and keep all individuals safe
- Keep students, staff and visitors safe while you are on the Academy site
- Keep accurate records of visits to the Academy
- Ensure that appropriate access arrangements can be provided for individuals that require them

Use of your personal data in automated decision making and profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Our lawful basis for using this data

Our lawful bases for processing your personal data for the purposes listed above are in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR).

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

- The data needs to be processed so that the Academy can fulfil a contract with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person e.g. to protect someone's life
- The data needs to be processed so that the Academy, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the Academy (where the processing is not for any tasks the Academy performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual has freely given clear consent

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Our basis for using special category data

For 'special category' data, we only collect and use it where we have both a lawful basis, as set out above, and one of the following conditions as set out in data protection law:

DATA PROTECTION AND GDPR

- We have obtained your explicit consent to use your 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 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 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 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

Collecting this data

While the majority of information we collect from you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from local authorities, government departments or agencies, police forces, courts or tribunals.

How we store this data

Personal data is stored in accordance with our Data Protection Policy.

DATA PROTECTION AND GDPR

We keep personal information about you while you work with our Academy. We may also keep it beyond your work with our Academy if this is necessary. The information is kept secure and is only used for purposes directly relevant to your work with the Academy.

We will retain and dispose of your personal information in accordance with the Information and Records Management Society's toolkit for schools.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

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

- The Academy sponsors (Diocese of Oxford, Buckinghamshire County Council)
- Government departments or agencies
- Local Authority – to meet our legal obligations to share certain information such as safeguarding concerns
- Our regulators [Ofsted, SIAMS]
- Non-Academy employees such as Governors, referees
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Our auditors
- Financial organisations
- Professional advisors and consultants
- Health and social welfare organisations
- Police forces, courts, tribunals

Transferring data internationally

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.

In cases where we have to set up safeguarding arrangements to complete this transfer, you can get a copy of these arrangements by contacting us.

Your rights

a. How to access personal information we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy holds about them.

DATA PROTECTION AND GDPR

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our Data Protection Officer.

b. Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data
- Prevent your data being used to send direct marketing
- Object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, have the personal data we hold about you deleted or destroyed, or restrict processing
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Data Protection Officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

DATA PROTECTION AND GDPR

Contact

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

Data Protection Officer
Kathy Buxton
Chiltern Hills Academy
Chartridge Lane
Chesham
Buckinghamshire
HP5 2RG
Email: dataprotection@chacademy.co.uk
Telephone: 01494 782066

This notice is based on The Key for School Leaders model Privacy Notice for suppliers of goods and services, amended to reflect the way we use data in Chiltern Hills Academy.