



ASPIRATIONS

HARRIERS BANBURY ACADEMY

UK GDPR- STAFF PRIVACY NOTICE

Version control	
UK GDPR- Staff Privacy Notice [2022-09-01]	Reviewed and updated to reflect reference to UK GDPR, and added reference to biometric data.
UK GDPR- Staff Privacy Notice [2021-04-01]	Reviewed and updated previous version to align with new DPO appointment.

Date of next review:	September 2024	Owner:	Director of HR & Compliance
Type of policy:	Trust	Approving Body:	Executive Operational Board

UK GDPR- STAFF PRIVACY NOTICE

Harriers Banbury Academy is committed to protecting the privacy and security of the personal information of staff. This privacy notice describes how personal information about staff is collected and used by the Academy during and after their period of working at the Academy, in accordance with the UK General Data Protection Regulation (UK GDPR).

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

This privacy notice applies to all current and former employees, workers and contractors.

Who collects this information?

Harriers Banbury Academy is a “data controller” and is therefore responsible for deciding how personal information about staff is held and used.

The Academy is required under data protection legislation to notify staff of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and the Academy may update this notice at any time.

It is important that staff members read this notice, together with any other privacy notice that may be provided on specific occasions when the Academy is collecting or processing personal information about them, so that they are aware of how and why such information is being used.

Data protection principles

The Academy will comply with the data protection principles when gathering and using personal information, as set out in its Data Protection Policy, which can be accessed from www.harriers-aspirations.org.

The categories of information that the Academy collects, processes, holds and shares

The Academy may collect, store and use the following categories of personal information about staff:

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Emergency contact information such as names, relationship, phone numbers and email addresses;
- Information collected during the staff recruitment process that is retained during a staff member's employment including references, proof of right to work in the UK, application form, CV, qualifications;
- Employment contract information such as start dates, hours worked, post, roles;
- Education and training details;
- Details of salary and benefits including payment details, payroll records, tax status information, national insurance number, pension and benefits information;

- Details of dependants;
- Nationality and immigration status and information from related documents, such as passport or other identification and immigration information;
- Information in sickness and absence records such as number of absences and reasons (including sensitive personal information regarding physical and/or mental health);
- Criminal records information as required by law to enable individuals to work with children;
- Trade union membership details;
- Information on grievances raised by a staff member or involving them;
- Information on conduct and/or other disciplinary issues involving a staff member;
- Details of appraisals, performance reviews and capability issues;
- Details of time and attendance records;
- Information about the use of the Academy's IT, communications and other systems, and other monitoring information;
- Details of a staff member's use of business-related social media;
- Images of staff captured by the Academy's CCTV system;
- Use of public social media (this is only in very limited circumstances, to check specific risks for specific functions within the Academy, and individuals will be notified separately if this is to occur);
- Details in references about a staff member received by the academy or given by the academy to others;
- Details of racial or ethnic origin, sex and sexual orientation, religious or similar beliefs.
- Recordings of staff from the Academy's video conferencing platform

How this information is collected

- The Academy may collect this information from staff members directly, from personnel records, the Home Office, pension administrators, staff members' doctors, from medical and occupational health professionals engaged by the Academy, the DBS, staff members' trade union, other employees, other professionals the Academy may engage (e.g. in an advisory capacity), automated monitoring of the Academy's websites and other technical systems such as our computer networks and connections, CCTV and access control systems, remote access systems, email and instant messaging systems, intranet and internet facilities.

How the Academy uses staff members' information

The Academy will only use personal information about staff members when the law allows it to. Most commonly, information will be used in the following circumstances:

-

- Where the Academy needs to perform the contract entered into with a staff member;
- Where the Academy needs to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for the Academy's legitimate interests (or those of a third party) and the interests, rights and freedoms of the relevant staff member do not override those interests.

- When consent to process personal data has been appropriately provided.

The Academy needs all the categories of information in the list above primarily to allow it to perform the contracts held with staff members and to enable the Academy to comply with legal obligations. Please note that the Academy may process information about a staff member without their knowledge or consent, where this is required or permitted by law.

The situations in which the Academy will process personal information about staff members are listed below:

- To determine recruitment and selection decisions on prospective employees;
- In order to carry out effective performance of the employee's contract of employment and to maintain employment records;
- To comply with regulatory requirements and good employment practice;
- To carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements;
- To enable the development of a comprehensive picture of the workforce and how it is deployed and managed;
- To enable management and planning of the workforce, including accounting and auditing;
- Personnel management including retention, sickness and attendance;
- Performance reviews, managing performance and determining performance requirements;
- In order to manage internal policy and procedure;
- Human resources administration including pensions, payroll and benefits;
- To determine qualifications for a particular job or task, including decisions about promotions;
- Evidence for possible disciplinary or grievance processes;
- Complying with legal obligations;
- To monitor and manage staff access to our systems and facilities in order to protect our networks, the personal data of our employees and for the purposes of safeguarding;
- To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution;
- Education, training and development activities;
- To monitor compliance with equal opportunities legislation;
- To answer questions from insurers in respect of any insurance policies which relate to a staff member;
- Determinations about continued employment or engagement;
- Arrangements for the termination of the working relationship;
- Dealing with post-termination arrangements;
- Health and safety obligations;
- Prevention and detection of fraud or other criminal offences; and
- To defend the Academy in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.

Further information on the monitoring undertaken by the Academy in the workplace and how this is done is available in other relevant policies, e.g., **Acceptable Use Policy**.

Some of the above grounds for processing will overlap and there may be several grounds which justify the Academy's use of staff members' personal information.

If a staff member fails to provide certain information when requested, the Academy may not be able to perform the contract that has been entered into with the individual (such as making salary payments or providing benefits), or the Academy may be prevented from complying with its legal obligations (such as to ensure the health and safety of its workers).

The Academy will only use personal information of staff for the purposes for which it has been collected, unless it reasonably considers that the information needs to be used for another reason and that reason is compatible with the original purpose. If the Academy needs to use a staff member's personal information for an unrelated purpose, the individual will be notified and provided with an explanation of the legal basis which allows the Academy to do so.

How the Academy uses particularly sensitive information

Sensitive personal information (as defined under the UK GDPR as "special category data") requires higher levels of protection and further justification for collecting, storing and using this type of personal information. The Academy may process this data in the following circumstances: -

- In limited circumstances, with the staff member's explicit written consent;
- Where the Academy needs to carry out its legal obligations in line with its data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to the Academy's pension schemes);
- Where it is needed to assess a staff member's working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, the Academy may process this type of information where it is needed in relation to legal claims or where it is necessary to protect a staff member's interests (or someone else's interests) and the staff member is not capable of giving their consent.

The Academy will use this information in the following ways: -

- Collecting information relating to leave of absence, which may include sickness absence or family related leave;
- To comply with employment and other laws;
- Collecting information about physical or mental health, or disability status, to ensure a staff member's health and welfare in the workplace and to assess their fitness to work, to provide appropriate workplace adjustments, to manage sickness absence and to administer benefits;
- Collecting information about race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- To record trade union membership information to pay trade union premiums and to comply with employment law obligations.

Criminal convictions

The Academy may only use information relating to criminal convictions where the law allows it to do so. This will usually be where it is necessary to carry out legal

obligations. The Academy will only collect information about criminal convictions if it is appropriate given the nature of the role and where it is legally able to do so.

Where appropriate the Academy will collect information about criminal convictions as part of the recruitment process or be notified of such information directly by staff members in the course of them working for the Academy.

Automated decision making

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. The Academy is allowed to use automated decision making in the following circumstances: -

- Where the Academy has notified the staff member of the decision and given them 21 days to request a reconsideration;
- Where it is necessary to perform the contract with a staff member and appropriate measures are put in place to safeguard their rights; or
- In limited circumstances, with the staff member's explicit written consent and where appropriate measures are in place to safeguard their rights.

Staff members will not be subject to decisions that will have a significant impact on them based solely on automated decision-making, unless the Academy has a lawful basis for doing so and have notified the relevant staff members.

Sharing data

The Academy may need to share data of staff members with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with the staff member or where the Academy has another legitimate interest in doing so. These include the following: -

- the Department for Education (DfE);
- Ofsted;
- other academies within the Trust;
- prospective employers;
- welfare services (such as social services);
- law enforcement officials such as police, HMRC;
- LADO;
- training providers;
- professional advisors such as lawyers and consultants;
- support services (including HR support, insurance, IT support, information security, pensions and payroll);
- The Local Authority;
- Occupational Health;
- DBS; and
- recruitment and supply agencies.

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations. The Academy requires them to respect the security of data and to treat it in accordance with the law.

Circumstances may arise where the Academy may transfer a staff member's personal information outside the EU. If the Academy does so, the individual can expect a similar degree of protection in respect of their personal information.

Retention periods

Except as otherwise permitted or required by applicable law or regulation, the Academy only retains personal data for as long as necessary to fulfil the purposes it was collected for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

To determine the appropriate retention period for personal data, the Academy considers the amount, nature, and sensitivity of personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for processing the personal data, whether the Academy can fulfil the purposes of processing by other means and any applicable legal requirements.

Once a staff member is no longer an employee, worker or contractor of the Academy, the Academy will retain and securely destroy the staff member's personal information in accordance with its data retention policy.

The Academy typically retains personal data for 6 years subject to any exceptional circumstances or to comply with laws or regulations that require a specific retention period.

Security

The Academy has put in place measures to protect the security of staff members' information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, the Academy limits access to staff members' personal information to those employees, agents, contractors and other third parties who have a business need to know.

Details of these measures are available from the **Information Security Policy**.

Third parties will only process personal information of staff members on instructions from the Academy and where they have agreed to treat information confidentially and to keep it secure.

The Academy has put in place procedures to deal with any suspected data security breach and will notify staff members and any applicable regulator of a suspected breach where it is legally required to do so.

Staff members' rights of access, correction, erasure and restriction

It is important that the personal information the Academy holds about staff members is accurate and current. Staff members are asked to keep the Academy informed if their personal information changes during their working relationship with the Academy.

Under certain circumstances by law staff members have the right to:

- Access their personal information (commonly known as a "subject access request"). This allows them to receive a copy of the personal information the Academy holds about them and to check the Academy is lawfully processing it. Staff members will not have to pay a fee to access their personal information. However, the Academy may charge a reasonable fee if a staff member's request for access is clearly unfounded or excessive. Alternatively, the Academy may refuse to comply with the request in such circumstances.

- Correct the personal information the Academy holds about them. This enables the staff member to have any inaccurate information the Academy holds about them corrected.
- Ask the Academy to delete or remove their personal data if there is no good reason for the Academy continuing to process it.
- Ask the Academy to suspend processing personal information about them in certain circumstances, for example, if they want the Academy to establish its accuracy before processing it.
- Object to processing in certain circumstances (for example for direct marketing purposes).
- Ask the Academy to transfer your personal information to another party.

Staff members wishing to exercise any of the above rights should contact The Principal in writing.

The Academy may need to request specific information to help confirm identity and ensure the right to access the information (or to exercise any other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where a staff member may have provided their consent to the collection, processing and transfer of their personal information for a specific purpose, they have the right to withdraw their consent for that specific processing at any time. To withdraw consent, please contact The Principal. Once the Academy has received notification that consent has been withdrawn, it will no longer process the staff member's information for the purpose or purposes that had originally been agreed, unless the Academy has another legitimate basis for doing so in law.

How to raise a concern

In the first instance, queries about the Academy's use of information about staff with The Principal.

The Academy has appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If queries about how the Academy handles personal information cannot be resolved by The Principal, then the DPO can be contacted as per the details below: -

Data Protection Officer: Judicium Consulting Limited
 Address: 72 Cannon Street, London, EC4N 6AE
 Email: dataservices@judicium.com
 Web: www.judiciumeducation.co.uk
 Lead Contact: Craig Stilwell

Staff members have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

Changes to this privacy notice

The Academy reserves the right to update this privacy notice at any time, and will provide a new privacy notice when making any substantial updates. The Academy may also notify staff in other ways from time to time about the processing of their personal information.