ASHLEY HIGH SCHOOL



Data Protection Policy and Privacy Notice

(General Data

Protection Regulation)

This policy was reviewed/updated: September 2023

Next review: September 2024

General Data Protection Regulation (GDPR) Policy

**1. INTRODUCTION**

1.1 The School is required to process personal data regarding staff, pupils and their parents and guardians and friends of the School relevant to its operation and shall take all reasonable steps to do so in accordance with this Policy. Processing may include obtaining, recording, holding, handling, disclosing, transportation, destroying or otherwise using data. In this Policy any reference to pupils, parents, friends or staff includes current past or prospective pupils, parents, friends or staff.

1.2 All staff are responsible for complying with this policy.

**2. SCOPE**

2.1 This Policy covers the School’s acquisition, handling and disposal of the personal and sensitive personal data it holds on all Staff, including temporary staff, agency workers, volunteers, parents and pupils. It also applies to Governors and contractors. It explains the School’s general approach to data protection which is to ensure that individual’s personal data and information is protected and appropriately processed and provides practical guidance which will help to ensure that the School complies with the Data Protection Act 1998 (the Act) and anticipates the General Data Protection Regulations 2018 (GDPR) which become law on 25thMay 2018.

**3. DEFINITIONS**

* 1. ***Personal data is:***
* Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
* This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
* The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.
* Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

***3.2 Sensitive personal data is:***

Any information about a person’s mental or physical health or condition, their political or religious beliefs, race, ethnicity, sexual life or orientation, trade union membership, criminal offences or alleged offences and any proceedings. **The GDPR refers to sensitive personal data as “special categories of personal data”.** The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual

The School has additional obligations in connection with the use of sensitive personal data, namely at least one of the following conditions must be satisfied:

1. Explicit consent of the data subject must be obtained
2. Necessary for carrying out the obligations under employment, social security or social protection law or a collective agreement
3. Used in connection with alumni relations provided it relates solely to this and there is no disclosure to a third party without consent
4. Data manifestly made public by the data subject
5. Various public interest situations as outlined in the General Data Protection Regulations 2018

***3.3 The data subject is:***

The person the information relates to. There may be more than one data subject, such as when a record concerns an incident involving two pupils.

***3.4 The Data Controller:***

The School is the Data Controller and is responsible for determining the purposes of its use of data - what data it gathers and how this information is used. As the Data Controller the School is responsible for complying with the Act.

***3.5 The Data Protection Officer:***

The School has appointed **Jonathan Greenough** **(Service Lead Officer, Halton LA)** as its Data Protection Officer, responsible for day to day compliance with this Policy. He can be contacted via the helpdesk by the following means:

**TEL: 0151 511 7002**

**EMAIL: schoolsdpo@halton.gov.uk**

**4. ACQUIRING, USING AND DISPOSAL OF PERSONAL DATA**

4.1 The School shall only process personal data for specific and legitimate purposes.

These are:

1. providing pupils and staff with a safe and secure environment including images on CCTV – all cameras around the School carry appropriate warning signs as to their operation. They are used for the purpose of detecting crime, ensuring personal security and the welfare of staff and pupils and the protection of the working environment. Images are kept no longer than 14 days to meet these objectives, however, in certain circumstances such as an on-going investigation into criminal activity certain relevant images may be kept for longer but no longer than necessary to complete any such investigation.
2. providing an education, training and pastoral care.
3. providing activities for pupils and parents - this includes school trips and activity clubs.
4. providing academic, examination and career references for pupils and staff.
5. protecting and promoting the interests and objectives of the School – this includes fundraising.
6. safeguarding and promoting the welfare of pupils.
7. monitoring pupils’ and staff’s email communications, internet and telephone use to ensure pupils and staff are following the School’s IT Acceptable Use policy.
8. promoting the School to prospective pupils and their parents.
9. communicating with former pupils.
10. for personnel, administrative and management purposes. For example to pay staff and to monitor their performance.
11. fulfilling the School's contractual and other legal obligations.

4.2 Staff should seek advice from the Data Protection Officer before using personal data for a purpose which is different from that for which it was originally acquired. If information has been obtained in confidence for one purpose, it shall not be used for any other purpose without the Data Protection Officer’s permission.

4.3 The School shall not hold unnecessary personal data, but shall hold sufficient information for the purpose for which it is required. The School shall record that information accurately and shall take reasonable steps to keep it up-to-date. This includes an individual's contact and medical details.

4.4 The School shall not transfer personal data outside the European Economic Area (EEA) without the data subject's permission unless it is satisfied that the data subject's rights under the Act will be adequately protected and the transfer has been approved by the Data Protection Officer. This applies even if the transfer is to a pupil's parents or guardians living outside the EEA.

4.5 When the School acquires personal information that will be kept as personal data, the School shall be fair to the data subject and fair to whoever provides the information (if that is someone else) in that their data will be handled and safeguarded in compliance with the Act.

4.6 The School shall only keep personal data for as long as is reasonably necessary and in accordance with the retention and disposal guidelines set out in the School’s Document Retention Policy. Staff should not delete records containing personal data without authorisation.

4.7 The School will keep personal data secure and adopt technical and organisational measures to prevent unauthorised or unlawful processing of personal data.

**5. INFORMATION AND EXPLANATION**

5.1 Privacy Notice: Individuals must be told what data is collected about them, and what it is used for. This is called a privacy notice or statement.

5.2 Purpose: The privacy notice is to ensure that the School’s collection and processing of personal data is done in a transparent way so it will explain who it applies to, why the information is being collected, what information will be collected how it will be acquired and processed, what it will be used for, which third parties (if any) it will be shared with, how long records will be retained for and outline the data subject’s rights, including the right to complain about the processing of their data to the Information Commissioner’s Office at Wycliffe House, Water Lane, Wilmslow. Cheshire SK9 5AF, telephone 0303 123 1113 or at: https://ico.org.uk/concerns/.

5.3 Staff are not expected to routinely provide pupils, parents and others with a privacy notice as this should have already been provided. Copies of the School’s privacy notice for pupils and parents can be obtained from the Data Protection Officer or accessed on the School’s website.

5.4 Use: Having said this, staff should inform the Data Protection Officer if they suspect that the School is using personal data in a way which might not be covered by an existing privacy notice. This may be the case where, for example, staff are aware that the School is collecting medical information about pupils without telling their parents what that information will be used for.

**6. PROTECTING CONFIDENTIALITY**

6.1 Disclosing personal data within the School: Personal data should only be shared on a need to know basis. Personal data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the School or their relationship to the data subject, unless they need to know it for a legitimate purpose. Examples include -  personal contact details for a member of staff (e.g. their home address and telephone number, and their private mobile telephone number and e-mail address) shall not be disclosed to parents, pupils or other members of staff unless the member of staff has given their permission.

6.2 Disclosing personal data outside of the School: Sharing personal data with others is often permissible so long as doing so is fair and lawful under the Act. However, staff should always speak to the Data Protection Officer if in doubt, or if staff are being asked to share personal data in a new way.

6.3 Before sharing personal data outside the School, particularly in response to telephone requests for personal data staff should:

a) make sure they are allowed to share it – that they have the necessary consent;

b) ensure adequate security. What is adequate will depend on the nature of the data. For example, if the School is sending a child protection report to social services on a memory stick then the memory stick must be encrypted; paper information should be sent by courier or recorded delivery, First or Second Class post is not considered secure enough and

c) make sure that the sharing is covered in the privacy notice.

6.4 The School should be careful when using photographs, videos or other media as this is covered by the Act as well. Specific guidance on this is provided in the School’s E-Safety policy on the School’s website.

6.5 Information security and protecting personal data: Information security is the most important aspect of data protection compliance and most of the fines under the Act for non-compliance relate to security breaches.

The School shall do all that is reasonable to ensure that personal data is not lost or damaged, or accessed or used without proper authority, and the School shall take appropriate steps to prevent these events happening. In particular:

1. paper records which include confidential information shall be kept in a cabinet or office which is kept locked when unattended.
2. the School uses a range of measures to protect personal data stored on computers, including file encryption, anti-virus and security software, sufficiently robust and frequently changed user passwords, audit trails and back-up systems.
3. staff must not remove personal data from the School's premises unless it is stored in an encrypted form on a password protected computer or memory device. Further information is available from the Data Protection Officer.
4. staff must not use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.

**7. DATA BREACHES**

7.1 Definition: A data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure or access to personal data.

7.2 Reporting obligations: Any actual data breach or alleged data breach must be reported to the Data Protection Officer as soon as it is discovered, whatever time that might be, to enable its circumstances to be investigated and appropriate action taken to limit any damage and to prevent a similar occurrence.

As soon as the School becomes aware of a significant data breach as determined by the Data Protection Officer it has 72 hours in which to report the breach to the Information Commissioner’s Office. Examples of breaches and their seriousness for reporting purposes are:

1. mistakenly sending an email or letter containing personal data to an incorrect recipient.
2. theft of IT equipment containing personal data.
3. failing to deal with a Subject Access Request.

If a breach is found to be sufficiently serious i.e. if not dealt with it is likely to result in a high risk to the rights and freedoms of individuals e.g. resulting in discrimination, damage to reputation, financial loss – through identity theft or otherwise – loss of confidentiality or any other significant economic or social disadvantage then not only does this breach have to be reported to the ICO within 72 hours of its discovery, the individuals concerned must be notified of the breach in a timely manner as directed by the Data Protection Officer.

**8. DATA SUBJECT’S RIGHTS, INCLUDING ACCESSING ANY DATA HELD ON THEM**

8.1 Individuals are entitled to know whether the School is holding any personal data which relates to them, what that information is, the source of the information, how the School uses it and who it has been disclosed to. This is known as a **Subject Access Request.**

Any member of staff wishing to exercise the right to request information covered by this policy, can do so by submitting a request in writing to the Data Protection Officer.

Any member of staff who receives a request for information covered by this policy from a pupil, parent or any other individual must inform the Data Protection Officer as soon as is reasonably possible, normally on the same day. This is important as there is a statutory procedure and timetable which the School must follow. Information must be provided to the requestor without delay and at the latest within one month of receipt.

8.2 Individuals have a right to ask the School not to use their personal data for direct marketing purposes or in ways which are likely to cause substantial damage or distress.

8.3 Individuals have a right to ask for incorrect personal data to be corrected or annotated.

8.4 Individuals have the right to object to any of their personal data being processed and to have this data erased.

8.5 Individuals have the right to restrict (halt) the processing of their personal data, usually whilst incorrect data is being corrected.

8.6 Individuals have the right to request their personal data is transferred to another data controller in a commonly used format.

8.7 Individuals have a right to ask the School not to make automatic decisions (using personal data) if such automatic decisions would affect them to a significant degree.

8.8 Individuals have the right to complain about the processing of their personal data to the Information Commissioner’s Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, Telephone 0303 123 1113 or at: <https://ico.org.uk/concerns/>.

**9. DATA PROCESSORS**

9.1 Where the school uses data processors (third parties / organisations that process (deals with or stores) personal data on the school’s behalf, the GDPR makes written contracts between the school and the processor a general requirement and that the contract must include certain specific terms as a minimum.  If the data processor then (with the school’s written authority) employs another processor, it also needs to have a written contract in place.

The school will check all existing contracts and if they do not contain all the requirements it will get new contracts drafted and signed as required.

The school will ensure data processors are communicated with so they understand :-

* + the reasons for the changes;
	+ the new obligations that GDPR put on them; and
	+ that they may be subject to administrative fines or other sanctions if they do not comply with new obligations.

**10. FURTHER INFORMATION**

10.1 The School has registered its use of personal data with the Information Commissioner's Office and further details of the Personal Data it holds, and how it is used, can be found in the School's register entry on the Information Commissioner's website at www.ico.gov.uk under registration number Z2975723 This website also contains further information about data protection.

**11. BREACH OF THIS POLICY**

11.1 A member of staff who deliberately or recklessly discloses personal data held by the School without proper authority is guilty of a criminal offence and gross misconduct.

This could result in summary dismissal.

**12. STATUS**

12.1 This policy is intended only as a statement of School policy. It does not form part of the contract of employment and may be amended from time to time.

**13. RELATED POLICIES include**:

IT Acceptable Use Policy

E-Safety Policy

Privacy Notice for Staff

Privacy Notice for Pupils and Parents

Document Retention Policy

**14. FURTHER INFORMATION**

14.1 If you require any further information and/or guidance regarding this policy, or its application, then please contact the school’s Data Protection Coordinator on 0151 424 4892, or via email at sec.ashley@haltonlearning.net

Further, and more detailed, information on data protection and how Halton Borough Council and DfE store and use personal information, can be obtained from the authority’s Data Protection Officer.

**Data Protection Officer**

**TEL: 0151 511 7002**

**EMAIL: schoolsdpo@halton.gov.uk**

Alternatively, please visit the following websites:

<http://www4.halton.gov.uk/Pages/Home.aspx>

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

If you cannot access these websites, please contact Halton Borough Council or the DfE as follows:

Janet Johnson – Information Governance – ICT Services – Halton Borough Council

Direct Dial Tel: 0151 511 7059 or via email janet.johnson@halton.gov.uk

DfE - Public Communications Unit Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT

Website: https://www.gov.uk/government/organisations/department-for-education

Email: http://www.education.gov.uk/help/contactus

Telephone: 0370 000 2288

**Privacy Notice**

**(How we use pupil information)**

**Why do we collect and use pupil information?**We collect and use pupil information under the General Data Protection Regulations (GDPR) which came into force on 25th May 2018.

*Article 6: Public task****:*** *the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law and

Article 9: Processing is necessary for reasons of substantial public interest, on the basis of law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;*

**Why we use the pupil data:**

* support pupil learning
* monitor and report on pupil progress
* provide appropriate pastoral care
* protect pupil welfare
* assess the quality of our services
* comply with the law regarding data sharing

**The personal data (categories of pupil information) that we collect, hold and share include:**

* Personal information (such as name, unique pupil number and address)
* Contact details, contact preferences, date of birth
* Special educational needs (SEND) information
* Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
* Attendance information (such as sessions attended, number of absences and absence reasons)
* Assessment information (including baseline and progress data)
* Relevant medical information
* Safeguarding information
* Exclusions/behavioural information
* Post-16 learning and destination information
* Photographs

**Collecting pupil information**

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if this is optional. If it is mandatory, we will explain the possible consequences of not complying.

**How we store this data**

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our Records and Retention Policy sets out how long we keep information about pupils. We hold pupil data for 9 years from when the pupil leaves.

**Data Sharing; who do we share pupil information with?**

We do not share information about pupils 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 pupils with the following third parties:

* Our local authority (Halton)
* The Department for Education (DfE)
* The pupil’s family and representatives
* Examining bodies
* Ofsted (as our regulator)
* Schools that pupils transition to when they leave us
* NHS services (eg. School nurse)

**Aged 14+ qualifications**

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

**Why we share pupil information**

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

We share pupils’ 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 pupils with our local authority (LA) and the Department for Education (DfE) under section 3 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 pupils aged 13+?**

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

* youth support services
* careers advisers

A parent / guardian can request that **only** 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 / pupil once he/she reaches the age 16.

**Our pupils aged 16+**

We will also share certain information about pupils 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 local authority website.

**The National Pupil Database (NPD)**

The NPD is owned and managed by the Department for Education and contains information about pupils 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 pupils 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 pupil information we share with the department, for the purpose of data collections, 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 pupils 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:

* 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 pupil 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 pupil 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>

**Requesting access to your personal data**

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child’s educational record, contact **sec.ashley@haltonlearning.net** who will inform the Data Protection Officer.

You also have the right to:

* object to processing of personal data that is likely to cause, or is causing, damage or distress
* prevent processing for the purpose of direct marketing
* object to decisions being taken by automated means
* in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
* claim compensation for damages caused by a breach of the Data Protection regulations

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

**Contact:**

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

* **The school: TEL 0151 424 4892 EMAIL:** **sec.ashley@haltonlearning.net**

OR

* **Data Protection Officer**

**TEL: 0151 511 7002**

**EMAIL:** **schoolsdpo@halton.gov.uk**

**Data Protection Officer**

**Halton Borough Council**

**Municipal Building**

**Kingsway**

**Widnes**

**WA8 7QF**

If you need information about how the Halton Borough Council and DfE store and use your information, then please go to the following websites:

http://www4.halton.gov.uk/Pages/Home.aspx

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

If you cannot access these websites, please contact Halton Borough Council or the DfE as follows:

Janet Johnson – Information Governance – ICT Services – Halton Borough Council

Direct Dial Tel: 0151 511 7059 or via email janet.johnson@halton.gov.uk

DfE - Public Communications Unit Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT

Website: https://www.gov.uk/government/organisations/department-for-education

Email: http://www.education.gov.uk/help/contactus

Telephone: 0370 000 2288

**Privacy Notice**

**(How we use information regarding the school workforce: those employed to teach, or otherwise engaged to work at, a school or a local authority)**

**The Data Protection Act 1998: How we use your information**

We process personal data relating to those we employ to work at, or otherwise engage to work at, our school. This is for employment purposes to assist in the running of the school and/or to enable individuals to be paid. The collection of this information will benefit both national and local users by:

* improving the management of workforce data across the sector
* enabling development of a comprehensive picture of the workforce and how it is deployed
* informing the development of recruitment and retention policies
* allowing better financial modelling and planning
* enabling ethnicity and disability monitoring; and
* supporting the work of the School Teachers’ Review Body

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

                   our local authority

                   the Department for Education (DfE)

If you need more information about how the Halton Borough Council and DfE store and use your information, then please go to the following websites:

* <http://www4.halton.gov.uk/Pages/Home.aspx>

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

If you want to see a copy of information about you that we hold, please contact:

* Sandra Collacott – sec.ashley@haltonlearning.net