
# Data Protection Policy

Last updated: 1 September 2019

Introduction

Hazel Wood High School holds personal data about employees, students, clients, suppliers and other individuals for a variety of business purposes

This policy outlines how the school seeks to protect personal data and ensure that staff **and governors** understand the rules governing the use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are always in place.

**Definitions**

| | |
|---|---|
| **Business purposes** | The purposes for which personal data may be used by us:<br><br>Personnel, administrative, financial, regulatory, payroll and business development purposes.<br><br>*School purposes include the following:*<br>- *Compliance with our legal, regulatory and corporate governance obligations and good practice*<br>- *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests*<br>- *Ensuring school policies are adhered to (such as policies covering email and internet use)*<br>- *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting*<br>- *Investigating complaints*<br>- *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments*<br>- *Monitoring staff conduct, disciplinary matters*<br>- *Marketing our school*<br>- *Improving services* |

| | |
|---|---|
| **Personal data** | Information relating to identifiable individuals and students, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.<br><br>*Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.* |
| Sensitive personal data | *Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.* |

**Scope**

This policy applies to all staff and governors working at Hazel Wood High School. Staff and governors must be familiar with this policy and comply with its terms.

This policy supplements other policies relating to Freedom of Information, Online Safety, CCTV, Safeguarding, and Anti-Bullying. We may supplement or amend this policy with additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff and ratified by governors.

**Our Procedure**

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual (whose details we are processing) has consented to this happening.

The Data Protection Officer's responsibilities:

- Keeping the senior leadership team updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, governors and other stakeholders
- Responding to individuals such as students, parents and employees who wish to know which data is being held on them.

- Checking and approving any contracts or agreements to ensure that they apply with the new data protection laws

Responsibilities of the IT Manager

- Ensure all systems, services, software and equipment meet acceptable security standard
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services (such as cloud services), that the school is considering using to store or process data

Responsibilities of the Business Manager

- Approving a data protection statement which is attached to all school emails
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the school's Data Protection Policy

The processing of all data must be**:**

- Necessary to deliver our service
- In our legitimate interests and not unduly prejudice the individual's private

Our Terms of Business contains a Privacy Notice to students/parents and staff on data protection.

The notice:

- Sets out the purposes for which we hold personal data on students and employee.
- Highlights that our work may require us to give information to third parties such as Department of Education, the Local Authority and other professional advisers
- States that students and staff have a right of access to the personal data that we hold about them

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that records can be updated.

Data security

Staff and governors must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it. It should not be left on desks, unsecure.
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly.

  Computers must be locked when leaving the room or the desk.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used.
- Data should not be sent to personal email accounts (to work with off-site). Always use work email accounts
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the school's backup procedures
- All mobile devices such as laptops, tablets or smartphones with data should have alpha numeric password protection.
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reason that the data was obtained, but should be determined in a manner consistent with the schools data retention guidelines.

Transferring data internationally

It should be noted that there are restrictions on international transfers of personal data. No one must not transfer personal data anywhere outside the UK without first consulting the Data Protection Officer.

**Subject access requests**

---

Please note that under the Data Protection Act 1998, individuals are entitled (subject to certain exceptions), to request access to information held about them.

Any subject access request, should be referred immediately to the DPO. Please follow steps outlined in

Appendix C and/or Appendix D.

Please contact the Data Protection Officer if you would like to correct or request any of your personal information. There are also restrictions on the information to which anyone is entitled to under applicable law.

Processing data in accordance with the individual's rights

All staff should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request

Do not send direct marketing material to someone electronically (e.g. via email) unless staff and governors have an existing business relationship.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

Training

All staff will receive training on this policy. New staff will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law, policy and/or procedure.

Training is provided in-house on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

**GDPR provisions**

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May

2018

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how Hazel Wood High School will use their personal data is important for our school.

Privacy Notices for parents and students can be found in Appendix A.
Privacy Notices for staff can be found in Appendix B.

Conditions for processing

Hazel Wood High School will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

Hazel Wood High School will process personal data in compliance with all six data protection principles.

1) Fair and Lawful
2) Purposes – only obtained for one or more specified and lawful purpose
3) Adequacy – relevant and not excessive in relation to the purpose or purposes for which it is processed
4) Accurate and kept up to date
5) Retention – not kept for longer than necessary
6) Rights

We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that Hazel Wood High School collects is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of personal data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that personal data is transferred directly to another system. This must be done free of charge.

Right to be forgotten

A data subject may request that any information held by our organisation is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the EEA before consultation with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures

- Notify the Information Commissioner's Office (https://ico.org.uk/concerns/) of any compliance failures that are material either in their own right or as part of a pattern of failures

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. The DPO will monitor it regularly to make sure it is being adhered to.

**Consequences of failing comply**

---

Staff and governors take compliance with this policy very seriously. Failure to comply puts both an individual and the school at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action which may result in dismissal. It should be noted that an individual can commit a criminal offence under, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the Data Controller.

If you have any questions or concerns about any aspect of this policy, do not hesitate to contact the DP

**Appendix A – Privacy Notice – How we use pupil information**

---

**Why do we collect and use pupil information?**

We collect and use pupil information under Article 6(1)(b) '*Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract,'* and article 9(2)(b) '*Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.'*

We use the pupil data:

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

**What is your 'Personal Data'?**

Personal data is information that says something about you as an individual, so it would normally include your name, and/or contact details, or even a photograph of you.

**The categories of parent information that we collect and hold include:**

- Personal information (names, addresses, contact numbers, email addresses, relationship).

**The categories of pupil information that we collect, hold and share include:**

- Student personal information (name, unique pupil number, date of birth, address, photograph, and religion)
- Parents/carers personal information (name, contact numbers, address, email address, work details [name, phone numbers, email address]).
- Characteristics (ethnicity, language, nationality, country of birth, free school meal eligibility, relevant medical information, biometrics)
- Education Information (Previous school(s), Special Educational Needs Information, National Curriculum Assessment results, Post 16 learning information)
- Attendance information (sessions attended, number of absences and absence reasons, exclusions/behavioural information)
- Welfare (In care details, child protection plans)

**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 you have a choice in this.

**Storing pupil data**

We hold pupil data till the pupil reaches the age of 25.

**Who do we share pupil information with?**

We routinely share pupil information with

- schools that the pupil's attend after leaving us
- educational websites
- outside agencies
- our local authority
- the Department for Education (DfE)

**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.

**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.

**Ourpupils 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 http://www.bury.gov.uk/index.aspx?articleid=10386.

**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 Daley Thompson (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

**Appendix B – Privacy Notices – The school Workforce**

---

**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, date of birth, gender, disabilities, and National Insurance numbers and characteristics such as ethnic group, Qualified Teacher Status, employment contracts and remuneration details, qualifications, absence information, and curriculum details.

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 require more information about how we and/or DfE store and use your personal data please visit:

- http://www.bury.gov.uk/index.aspx?articleid=10637
- 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 the school.

## Appendix C – Subject access request record

---

**Subject access request record**

Name of data subject: _____

Name of person who made request: _____

Date request received: ___/___/____

Contact DPO:

___/___/____

Date acknowledgement sent:

Name of person dealing with request: _____

**Guidance Process**

Are they entitled to the data?

*Do you understand what data they are asking for? If no reply stating reasons and/or ask for proof*

*If no, ask requestor for clarity*

Identify the data

*What data sources, where are they kept*

Collect the data required.

*Do you own all the data?*

*Do you need to except/redact data?*

*Is the data going to be ready in time?*

*You may need to ask others - state a deadline in your request*

*If no, ask third parties to release external data.*

*If data is supplied by another agency such as the Psychology Service, we do not own the data.*

*If exempting/redacting be clear of your reasons. Document name, data exempted/redacted, why.*

Record delays and reasons.

Communicate with requestor stating reasons for delay and asking if they would like the data you have collected so far.

Create pack.

Make sure that the data is in an easy to access format: paper, word, excel (csv), etc. Make a copy to keep.

Inform requestor you have the data.

Deliver data

*Ask them how they would like it delivered.*

*Ask for confirmation/special deliver*

At all stages, your DPO will be able to provide you with advice

Date request completed: (within 30 days of request)

Signed off by: _____ Date

## Appendix D – Letter template for refusal of a request

…./……/20……

Dear ……..

I am writing to you to let you know your request for information from Hazel Wood High School relating to…….. requested on ……/……../20..... has been denied.

We have denied access to this information because

……
……

……

Please be aware that if you are not satisfied with the reasons listed above, and you would like to discuss this matter further, please contact school.

In addition, you have the right to complain to the Information Commissioner's Office (ICO) and also to seek judicial remedy, if you so wish.

Yours sincerely

Data Protection Officer