Hodge Hill College

# Data Protection Policy

| | |
|---|---|
| **Approved On/By:** | Staffing, Premises & Finance Committee 7th February 2024 |
| **Last Reviewed On:** | 30th January 2024 |
| **Next Review Due By:** | Staffing, Finance and Premises Spring term 2025 |
| **Monitoring & Review:** | Annually |
| **Staff Member(S) Responsible:** | S Butt |

**Data Protection Policy**
**Contents**

## 1 Policy statement

1.1 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as a School we will collect, store and **process personal data** about our pupils, **workforce**, governors, visitors, parents and others. This makes us a **data controller** in relation to that **personal data**.

The school is registered with the ICO/ has paid its data protection fee to the ICO, as legally required

1.2 We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.3 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.4 All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

## 2 About this policy

2.1 The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('**GDPR**'), the [Data Protection Act 2018], and other regulations (together '**Data Protection Legislation**').

2.2 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

2.5 This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK 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 guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

## 3 Definition of data protection terms

3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

## 4 Roles and Responsibilities

Data Protection Officer

4.1 As a School we are required to appoint a Data Protection Officer ("DPO"). Our DPO is Mrs S Butt, and she can be contacted at Hodge Hill College, Bromford Road, Birmingham B36 8HB.

4.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

4.3 The DPO will provide an annual report of their activities directly to the Governing Body and, where relevant report to the board their advice and recommendations on school data protection issues.

4.4 The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

4.5 advising school leaders and staff about their data obligations

4.6 monitoring compliance

4.7 conducting regular data audits

4.8 developing and updating data protection policies and procedures

4.9 monitoring who in the school has access to personal data

4.10 advising when data protection impact assessments are needed

4.11 answering data protection enquiries from staff, parents and pupils

4.12 making sure privacy notices are regularly reviewed and updated

4.13 supporting and advising staff who have data protection queries

4.14 communicating with the Information Commissioner's Office (ICO)

4.15 reporting to the governing board or trustees about data protection

4.16 advising the governing board or trustees on data protection risks

4.17 advising on and co-ordinating responses to information rights requests

4.18 making sure all assets containing personal data are appropriately managed and secure

**Headteacher**

4.19 The Headteacher acts as the representative of the data controller on a day-to-day basis

**Senior leaders are accountable for:**

4.20 Deciding how the school uses technology and maintains its security

4.21 deciding what data is shared and how

4.22 setting school policies for the use of data and technology

4.23 understanding what UK GDPR and the Data Protection Act covers and getting advice from the data protection officer, as appropriate

4.24 assuring governors and trustees that the school has the right policies and procedures in place

4.25 making sure any contracts with third-party data processors cover the relevant areas of data protection

**5** making sure staff receive annual training on data protection, including specific school processes such as personal data breach reporting processes and the escalation of information rights requests

**Governing Board**

5.1 The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations

5.2 Monitors their date protection performance

5.3 Support the data protection officer

5.4 Has good network security infrastructure to keep personal data protected

5.5 Has a business continuity plan in place that includes cybersecurity

**All Staff**

5.6 All Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school 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 UK
    - 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

6.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

6.1.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**;

6.1.2 **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;

6.1.3 Adequate, relevant and not excessive for the purpose;

6.1.4 Accurate and up to date;

6.1.5 Not kept for any longer than is necessary for the purpose; and

6.1.6 **Processed** securely, using appropriate technical and organisational measures.

6.2 **Personal Data** must also:

6.2.1 be **processed** in line with **data subjects'** rights;

6.2.2 not be transferred to people or organisations situated in other countries without adequate protection.

6.3 We will comply with these principles in relation to any **processing** of **personal data** by Hodge Hill College.

## 7 Fair and lawful processing

7.1 Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.

7.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

7.2.1 that the **personal data** is being **processed**;

7.2.2 why the **personal data** is being **processed**;

7.2.3 what the lawful basis is for that **processing** (see below);

7.2.4 whether the **personal data** will be shared, and if so with whom;

7.2.5 the period for which the **personal data** will be held;

7.2.6 the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and

7.2.7 the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

7.3 We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

7.4 For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:

7.4.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;

7.4.2 where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g the Education Act 2011);

7.4.3 where the **processing** is to ensure the vital interests of the individual or another person i.e. to protect someone's life

7.4.4 where the data needs to be processed so that the school, as apublic authority, can perform a task in the public interest or exercise its official authority

7.4.5 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data.**

7.5 When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:

7.5.1 where the **processing** is necessary for employment law, social security or social protection law purposes, for example in relation to sickness absence;

7.5.2 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;

7.5.3 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and

7.5.4 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.

7.6 We will inform **data subjects** of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

7.7 If any **data user** is in doubt as to whether they can use any **personal data** for any purpose then they must contact the DPO before doing so.

**Vital Interests**

7.8 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

**Consent**

7.9 Where none of the other bases for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

7.10 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

7.11 When pupils and/or our Workforce join Hodge Hill College a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete provide consent

7.12 In relation to all pupils under the age of [12/13] years old we will seek consent from an individual with parental responsibility for that pupil.

7.13 We will generally seek consent directly from a pupil who has reached the age of [12/13], however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

7.14 If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must:

7.14.1 Inform the **data subject** of exactly what we intend to do with their **personal data**;

7.14.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and

7.14.3 Inform the **data subject** of how they can withdraw their consent.

7.15 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.

7.16 The DPO must always be consulted in relation to any consent form before consent is obtained.

7.17 A record must always be kept of any consent, including how it was obtained and when.

## 8 Processing for limited purposes

8.1 In the course of our activities as a School, we may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our **workforce**).

8.2 We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

## 9 Notifying data subjects

9.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

9.1.1 our identity and contact details as **Data Controller** and those of the DPO;

9.1.2 the purpose or purposes and legal basis for which we intend to **process** that **personal data**;

9.1.3 the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;

9.1.4 whether the **personal data** will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place;

9.1.5 the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy;

9.1.6 the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and

9.1.7 the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

9.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

**10 Adequate, relevant and non-excessive processing**

10.1 We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

**11 Accurate data**

11.1 We will ensure that **personal data** we hold is accurate and kept up to date.

11.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

11.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

**12 Timely processing**

12.1 We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.

**13 Processing in line with data subject's rights**

13.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

13.1.1 request access to any **personal data** we hold about them;

13.1.2 object to the **processing** of their **personal data**, including the right to object to direct marketing;

13.1.3 have inaccurate or incomplete **personal data** about them rectified;

13.1.4 restrict **processing** of their **personal data**;

13.1.5 have **personal data** we hold about them erased

13.1.6 have their **personal data** transferred; and

13.1.7 object to the making of decisions about them by automated means.

- **The Right of Access to Personal Data**

13.2 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the schools Subject Access Request Procedure.

- **The Right to Object**

13.3 In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

13.4 An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

13.5 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

13.6 In respect of direct marketing any objection to **processing** must be complied with.

13.7 The School is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

- **The Right to Rectification**

13.8 If a **data subject** informs Hodge Hill College that **personal data** held about them by the School is inaccurate or incomplete then we will consider that request and provide a response within one month.

13.9 If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the **data subject** within one month of their request that this is the case.

13.10 We may determine that any changes proposed by the **data subject** should not be made. If this is the case then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

- **The Right to Restrict Processing**

13.11 **Data subjects** have a right to "block" or suppress the **processing** of **personal data**. This means that the School can continue to hold the **personal data** but not do anything else with it.

13.12 Hodge Hill College must restrict the **processing** of **personal data**:

13.12.1 Where it is in the process of considering a request for **personal data** to be rectified (see above);

13.12.2 Where the school is in the process of considering an objection to processing by a **data subject**;

13.12.3 Where the **processing** is unlawful but the **data subject** has asked the School not to delete the **personal data**; and

13.12.4 Where the School no longer needs the **personal data** but the **data subject** has asked the School not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the School.

13.13 If Hodge Hill College has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

13.14 The DPO must be consulted in relation to requests under this right.

- **The Right to Be Forgotten**

13.15 **Data subjects** have a right to have **personal data** about them held by Hodge Hill College erased only in the following circumstances:

13.15.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected;

13.15.2 When a **data subject** withdraws consent – which will apply only where the School is relying on the individuals consent to the **processing** in the first place;

13.15.3 When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;

13.15.4 Where the **processing** of the **personal data** is otherwise unlawful;

13.15.5 When it is necessary to erase the **personal data** to comply with a legal obligation; and

13.16 Hodge Hill College is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

13.16.1 To exercise the right of freedom of expression or information;

13.16.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;

13.16.3 For public health purposes in the public interest;

13.16.4 For archiving purposes in the public interest, research or statistical purposes; or

13.16.5 In relation to a legal claim.

13.17 If Hodge Hill College has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

13.18 The DPO must be consulted in relation to requests under this right.

- **Right to Data Portability**

13.19 In limited circumstances a **data subject** has a right to receive their **personal data** in a machine readable format, and to have this transferred to other organisation.

13.20 If such a request is made then the DPO must be consulted.

## 14 Data security

14.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.

14.2 We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction.

14.3 Security procedures include:

14.3.1 **Entry controls.** Any stranger seen in entry-controlled areas should be reported to the Site Team

14.3.2 **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind and be kept within the retention guidelines(Personal information is always considered confidential.)

14.3.3 **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets and by a certified company with the ADISA accreditor

14.3.4 **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock their PC when it is left unattended and log off at the end of the day

**14.3.5 Working away from the school premises –** paper documents must be kept in a secure environment

14.3.6 **Working away from the school premises – electronic working.**

(a) Access to work should be from a secure network provided by the school

(b) No USB sticks are to be used. No data/personal information should be downloaded onto personal devices.

(c) Any work should be accessed using FOLDR and edited in FOLDR and through the school website / through authorised school VPN connection

(d) Downloading any form of personal data onto personal devices including mobile phones, laptops and ipads or USB sticks and memory devices is prohibited

(e) You are allowed to download data onto a school device as these are devices are encrypted and password protected

14.3.7 **Document printing.** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

14.3.8 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.

14.3.9 In particular:

14.3.10 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

14.3.11 Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access. A clear desk policy is in place for all staffing personnel

14.3.12 Passwords are at least 8 characters long containing upper/lower case characters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals

14.3.13 Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

14.3.14 Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our online safety policy/acceptable use agreement

14.3.15 Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is transported securely and adequately protected. Ensure the recipient is authorised and correct at the time of sending the email. (see section 8)

14.3.16 We use an external company to backup our files and folders on a daily basis. The data is encrypted end to end and an encryption key is required to perform any file restoration. The company is GDPR compliant and has accreditation for the following ISO9001, ISO27001 and 22301. This cloud solution works alongside our Business Continuity Plan.

14.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

## 15 Data Protection Impact Assessments

15.1 Hodge Hill College takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities

whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

15.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

15.3 Hodge Hill College will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

15.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

## 16 Disclosure and sharing of personal information

We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

16.1 Hodge Hill College will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence or there is an issue with a pupil or parent/carer that puts the safety of our staff at risk.

16.2 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

16.3 Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor 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

16.4 Where we transfer personal data internationally, we will do so in accordance with UK data protection law

16.5 We may also share personal data with emergency services and local authorities to help them respond to an emergency situation that affects any of our staff or pupils.

16.6 Further detail is provided in our Schedule of Processing Activities.

## 17 Data Processors

17.1 We contract with various organisations who provide services to the School, including:

Payroll providers, website hosts, catering contractors, educational consultants, text messaging services,

17.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

17.3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the School. Hodge Hill College will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

17.4 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

## 18 Images and Videos

18.1 Parents and others attending School events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. Hodge Hill College does not prohibit this as a matter of policy.

18.2 Hodge Hill College does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the School to prevent.

18.3 Hodge Hill College asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

18.4 As a School we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

18.5 Whenever a pupil begins their attendance at Hodge Hill College they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

## 19 CCTV & Body Worn Devices

Hodge Hill College operates a CCTV system. We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

- 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 Mr D Abbas– ICT Manager. Please refer to the School CCTV Policy inclusive of Body Worn Devices policy.

## 20 Biometric recognition Systems

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

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

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school 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 pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using a pin code at each transaction if they wish.

Parents/carers and pupils 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 pupil 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 pupil's parent(s)/carer(s).

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

## 21 Data security and 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 securely when not in use
- 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. School has a clear desk policy
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils 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
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned

equipment (see our acceptable use policy for staff and pupils and the BCC E safety policy)

- 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.

## 22 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 school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law

## 23 Personal data breaches

The school 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 annex 2.

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 school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

## 24 Training

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

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

## 25 Changes to this policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

**ANNEX 1**

**DEFINITIONS**

| Term | Definition |
|---|---|
| Data | is information which is stored electronically, on a computer, or in certain paper-based filing systems |
| Data Subjects | for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information |
| Personal Data | means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person |
| Data Controllers | are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes |
| Data Users | are those of our workforce (including Governers and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times |
| Data Processors | include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions |
| Processing | is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties |
| Special Category Personal Data | includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data |
| Workforce | Includes, any individual employed by Hodge Hill College such as staff and those who volunteer in any capacity including Governors, parent helpers, volunteers |

**Annex 2: Personal data breach procedure**

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (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

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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) before and after the implementation of steps to mitigate the consequences

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:

A description of the nature of the personal data breach including, where possible:

  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. 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

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to 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

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

## Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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.

Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your school. For example:

### 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 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 attempt to recall it from external recipients and

remove it from the school's email system (retaining a copy if required as evidence)

- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to 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 endeavor to obtain 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
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- Hardcopy reports sent to the wrong pupils or families