Harrison College Ltd

Data Protection Policy

Reviewed: October 2023
Updated: February 2024
Next Review: February 2025

Aims

Harrison College aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data and CCTV . It also reflects the ICO's code of practice for the use of surveillance cameras https://www.gov.uk/government/publications/update-to-surveillance-camera-code and personal information. In addition, this policy complies with our funding agreement and articles of association.

The public have a right to complain and this can be lodged with the ICO Make a complaint | ICO

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Health – physical or mental • Sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Champion	Principal
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The data controller

Harrison College processes personal data relating to parents, students, staff, directors, visitors and others, and therefore is a data controller.

Harrison College is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles and responsibilities

This policy applies to **all staff** employed by Harrison College, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing board

The Board of Directors has overall responsibility for ensuring that Harrison College complies with all relevant data protection obligations.

Data Protection Officer

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

They will provide an annual report of their activities directly to the Board of Directors and, where relevant, report their advice and recommendations on school data protection issues.

The DPO is first point of contact for individuals whose data Harrison College processes. The DPO is Harrison College's key contact for the ICO.

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

Our DPO is Gemma Peebles and is contactable via: principal@harrisoncollege.co.uk

The Principal/CEO

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

All staff

All staff are responsible for:

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

Data protection principles

The GDPR is based on data protection principles that Harrison College must comply with.

The principles say that personal data must be:

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

This policy sets out how Harrison College aims to comply with these principles.

Collecting personal data

1. **Lawfulness, fairness and transparency**
   We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:
   - The data needs to be processed so that Harrison College can fulfil a contract with the individual, or the individual has asked Harrison College to take specific steps before entering into a contract
   - The data needs to be processed so that Harrison College can comply with a legal obligation
   - The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
   - The data needs to be processed so that Harrison College, as a public authority, can perform a task in the public interest, and carry out its official functions
   - The data needs to be processed for the legitimate interests of Harrison College or a third party (provided the individual's rights and freedoms are not overridden)
   - The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent

   For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

   Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. The right to be informed, to have access and to have the data erased is followed.

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

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

   Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with Harrison College's Records Management and Retention Policy and Schedule.

Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent where necessary before doing this
  - This will be done through secure platforms such as CPOM's and SIMS and the SCR

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

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including but not limited to for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff. The use of encryption and secure password protected platforms are used in these cases.

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

Subject access requests and other rights of individuals

1. **Subject access requests**

   Individuals have a right to make a 'subject access request' to gain access to personal information that the College holds about them. This includes:

   - Confirmation that their personal data is being processed
   - Access to a copy of the data
   - The purposes of the data processing
   - The categories of personal data concerned
   - Who the data has been, or will be, shared with
   - How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
   - The source of the data, if not the individual
   - Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

   Subject access requests must be submitted in writing where possible, either by letter, email or fax to the DPO. They should include:

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

   If staff receive a subject access request, they must immediately forward it to the DPO.

2. **Children and subject access requests**

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

   Children below the age of 16 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our College may be granted without the express permission of

the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 16 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our College may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

3. Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will normally provide the information free of charge unless it falls under *'a reasonable fee'
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

4. Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Parental requests to see the educational record

Parents, or those with parental responsibility, can have access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request. A written request must be made to the College's Data Champion (DPO/Principal).

CCTV

We use CCTV in the interior of the College to ensure we remain safe. There are notices displayed near the areas of the cameras in accordance with Article 13. The use of CCTV is for safeguarding reasons as well as security to maintain the safety of our students and staff community.

The reviewing of CCTV is used only in rare cases where it is necessary, and only in the designated areas where confidentiality can be maintained. The review of any material will be carried out by the designated people only. The capacity to record sound is switched off.

Examples of when CCTV playback may be viewed would be:

- An accusation of physical violence or aggression from a student or member of staff
- An accusation of gross misconduct from a student regarding a member of staff
- An accusation of an unlawful act, such as theft regarding a student or member of staff
- An incident where an intruder enters the building, and the recording is used in a criminal investigation

We do not need to ask individuals' permission to use CCTV. The security (CCTV) cameras are clearly visible and fixed. The staff handbook informs staff of the use and purpose of CCTV monitoring. The college has signs in place near to all cameras to inform all college user's including visitors to the site, that CCTV is in use.

The designated person(s) for viewing CCTV monitoring are G Peebles (Principal) and G Stonier (Safeguarding DSL and Director).

Any enquiries about the CCTV system should be directed to the Data Protection Officer in the first instance.

Photographs and videos

As part of our College activities, we may take photographs and record images of individuals. We obtain written consent from parents/carers, or students aged 16 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials, via the permissions letter which is included in the 'welcome pack'.

Uses may include but are not limited to:

- Within College on notice boards and in College magazines, brochures, newsletters, etc.
- Outside of College by external agencies such as the College photographer, newspapers, campaigns
- Online on the College's website or social media pages

Photographs or video's taken by parents or carers at school events on their own personal devices are exempt from the DPA regulations at Harrison College. Information and guidance is given to students, parents and employers about the safe and correct use of photo's, video's and sharing of information, before events of these nature take part.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. Personal data will not be attributed to the photo's or video's without the prior consent of the person involved.

Live streaming

Live streaming of lessons, through Microsoft Teams or Google platform may also be used in rare cases such as Self Isolation and Co-vid related absences. All staff have been trained on the safe use and on-line digital technology and have completed NOS certification in this area.

Student and parent information video's on the safe use and rules and regulations concerning personal data and information have been circulated.

Recording of sessions is not permissible unless permission to do so has been agreed by the Principal beforehand. All participants will be informed of any recording and can withdraw consent at any time within the session.

See the College's Safeguarding and Child Protection Policy for more information on our use of photographs and videos. The ICT safe use policy explains our expectations in more detail.

Data protection by design and default

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

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

A data protection impact assessment will be carried out annually, or reviewed earlier if there is a cause to do so such as a near miss breach or complaint.

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 under lock and key when not in use

- 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
- In exceptional circumstances where personal information needs to be taken off site, staff must adhere at all times to the data protection regulations and comply with this policy. Failure to do so may result in a disciplinary
- Passwords that are at least 8 characters long containing letters and numbers are used to access College computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Staff, students or Directors, wherever possible, should be using the remote access system provided. If they ever store personal information on their personal devices, then they are expected to follow the same security procedures as for College-owned equipment (see our IT Acceptable Use Agreement)
- 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

The college uses CPOM's and SIMS as its regulated management information systems. Staff are trained in the safe use of these platforms.

Permissions and confidentiality limits are placed on both systems with authorised persons allowed full area access. This is limited to the Principal, Safeguarding lead, DSL and the Chief Operating Officer.

The DPO has a level of permission to allow them to carry out the functions of their job description and that of the DPO role.

Two factor authentication, passwords and encryption are used on all devices to ensure appropriate security. Staff and students are inducted, trained and receive regular updates on safe use and security.

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 College's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law and the College's Records Management and Retention Policy and Schedule. On leaving the College as an employee, we will delete or shred data after a period of 3 months. Some information may be held by our external processor and may be accessed under certain requirements.

Personal data breaches

Harrison College will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

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

Training

All staff and Directors 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 College's processes make it necessary.

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary – if any changes are made to the bill that affect our College's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the Board of Directors.

Links with other policies

This Data Protection Policy is linked to our:

- Privacy Policy
- Acceptable use of ICT
- Remote Learning: ICT Acceptable Usage Policy (and agreement)
- Child protection and Safeguarding Policy
- IT Acceptable Use Agreement
- IT Information Security Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Principal
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

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

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored GDPR.CO.UK
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - 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 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 GDPR.CO.UK

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

Actions to minimise the impact of data breaches

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

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