# Data Protection Policy

Heart of Yorkshire Education Group

## Contents


Policy Statement....3
Definitions....4
Introduction to Data Protection....6
The Principles of Data Protection....6
Accountability and Transparency....6
1. Fair and Lawful Processing....8
1.1 Controlling vs. processing data....8
1.2 Lawful Basis for Data Processing....8
1.3 Deciding which condition to rely on....9
2. Responsibilities....9
2.1 Our Responsibilities....9
2.2 Your Responsibilities....10
2.3 Responsibilities of the Data Protection Officer....11
2.4 Accuracy and relevance....11
2.5 Retention....11
2.6 Transfers of data....11
2.7 Data Security and Breach Reporting....12
3. The Rights of Individuals....13
3.1 Right to be informed....13
3.2 Right of access....13
3.3 Right to rectification....13
3.4 Right to erasure....13
3.5 Right to restrict processing....14
3.6 Right to data portability....14
3.7 Right to object....14
3.8 Rights related to automated decision making....14
4. Privacy Notices....15
4.1 When to supply a privacy notice....15
4.2 Contents of a privacy notice....15
4.3 How to supply a privacy notice....15
5. Subject Access Requests....16
5.1 How we deal with subject access requests....16
6. Requests for erasure....16
6.1 How we deal with requests for erasure....16
7. Third parties....17

7.1 Using third party controllers and processors ..... 17
7.2 Contracts ..... 17
8. Data Breaches ..... 18
8.1 Legal obligation to report breaches ..... 18
9. Complaints against the DPO ..... 18
9.1 How we deal with complaints against the DPO ..... 18
10. Audits, monitoring and training ..... 19
10.1 Data audits ..... 19
10.2 Monitoring ..... 19
10.3 Training ..... 19
Appendices ..... 20
Appendix 1: ICO Registration ..... 20
Appendix 2: Privacy Statement Examples ..... 21
Appendix 3: Subject Access Request form ..... 22
Appendix 4: Data Protection awareness declaration ..... 23
Appendix 5: Key Contacts ..... 24

# Policy Statement

This policy applies to the processing of all personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system, where that data is under the direct or indirect control of the College.

The purpose of this policy is to set out rules for governing the handling of personal data in relation to the College's current and former staff (including employees, temporary and agency workers, interns, volunteers and apprentices) and students and suppliers, and other individuals, thereby providing a code of good information handling practice and ensuring that all requirements of data protection legislation are met.

This policy applies to all staff of the College and its agents, volunteers, and contractors, while involved in any way with processing of data where the College is defined as the data controller.

All employees should be aware of, and should abide by, their obligations under this policy and data protection legislation. Any breach of data protection legislation or this policy could result in legal and/or disciplinary proceedings being taken against the responsible individual.

The implementation of this policy is the responsibility of each and every employee.

A copy of this policy must be made available on the College intranet/internet.

# Definitions

| | |
|---|---|
| binding corporate rules (BCRs) | BCRs are designed to allow multinational companies to transfer personal data from the European Economic Area (EEA) to their affiliates located outside of the EEA. They must be applied for, and approved by, an appropriate supervisory authority. For UK based institutions this is likely to be the ICO. |
| 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>*Business 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 business policies are adhered to (such as policies covering email and internet use), operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking*<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 business*<br>- *Improving services.* |
| College | means Heart of Yorkshire Education Group |
| data controller | means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law. |
| data processor | means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. |
| data protection legislation | The current enforceable legislation in UK law governing data protection. |
| data subject | means the individual to whom the personal information relates. |
| DPO | means the Data Protection Officer, the legally designated individual within an organisation that has defined roles and responsibilities under GDPR. Under certain circumstances, some organisations are mandated to appoint a DPO: the College falls under one of these circumstances as a Public Authority. |
| European Economic Area (EEA) | The European Economic Area (EEA) is the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market. For further information and a current list of member states see https://www.gov.uk/eu-eea |

| | |
|---|---|
| GDPR | Regulation (EU) 2016/679 as defined by the EU Parliament in April 2016. The regulation governs the processing of personal data relating to data subjects resident or ordinarily resident in the EU. |
| personal data | means any information relating to an identified or identifiable natural person ('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.<br><br>*Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.* |
| processing | means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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. |
| special categories of personal data | Special categories of data include information 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, and genetic and biometric information — any use of special categories of personal data should be strictly controlled in accordance with this policy. |
| supervisory authority | This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioner's Office (ICO). |
| We/us/our etc. | Are references to the College. |

# Introduction to Data Protection

The College is committed to protecting the rights and freedoms of Data Subjects and safely and securely processing their data in accordance with all of our legal obligations.

We hold personal data for a variety of business purposes. Data on personnel and payroll records has long been seen as confidential, but information about students is routinely used by College staff in many ways. All personal data, whether recorded on the College's information systems, on personal computers, or in manual filing systems, are data that must be treated with as much care as other more obviously 'confidential' data.

The College is registered with the supervisory authority as a data controller (please see Appendix 1). However, data protection legislation requires much more than simple registration: it places numerous obligations on people and organisations that record and use personal data. They must be open about that use and, in particular, comply with the six data protection principles by following sound and proper practices.

## The Principles of Data Protection ("Principle(s)")

1. **Lawful, fair and transparent**
   Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.
2. **Limited for its purpose**
   Data can only be collected for a specific purpose.
3. **Data minimisation**
   Any data collected must be necessary and not excessive for its purpose.
4. **Accurate**
   The data we hold must be accurate and kept up to date.
5. **Retention**
   We cannot store data longer than necessary.
6. **Integrity and confidentiality**
   The data we hold must be kept safe and secure.

## Accountability and Transparency

We must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. The College is responsible for keeping a written record of how all the data processing activities we are responsible for comply with each of the Principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency principle of GDPR, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security and enhanced privacy procedures on an ongoing basis.

Failure to comply with data protection legislation or this policy document could result in legal and/or internal disciplinary proceedings. It should be noted that contravention of data protection legislation might carry a personal as well as a corporate liability.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the DPO be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

For further information or guidance in relation to data protection matters contact the DPO. Contact details for the DPO and other persons of note referenced in this policy can be found in Appendix 5: Key Contacts.

# 1. Fair and Lawful Processing

## 1.1 Controlling vs. processing data

1.1.1 The College is classified as a data controller and data processor. We must maintain our appropriate registration with the supervisory authority in order to continue lawfully controlling and processing data.

1.1.2 As a data processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller(s). If at any point we determine the purpose and means of processing, we shall be considered a data controller and would gain the same legal liability as the controller. As a data processor, we must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches.

1.1.3 If you are in any doubt about how we handle data, contact the DPO for clarification.

1.1.4 Both data controllers and data processors are responsible for compliance with the Data Protection Act 2018, and as such are both liable for any data breaches for which they are responsible.

## 1.2 Lawful Basis for Data Processing

1.2.1 We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This means that we should not process personal data unless we have a lawful basis to do so.

1.2.2 We must establish a lawful basis for each data processing activity. If we cannot apply a lawful basis, our processing does not conform to the first Principle and will be unlawful. Ensure that any data you are responsible for managing has a written lawful basis approved by the DPO. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply the lawful basis. At least one of the following conditions must apply whenever the College processes personal data:

- **Contract**
  The processing is necessary to fulfil or prepare a contract for the individual.
- **Legal Obligation**
  We have a legal obligation to process the data (excluding a contract).
- **Vital Interest**
  Processing the data is necessary to protect a person's life or in a medical situation.
- **Legitimate Interest**
  The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest, or where the processing is undertaken in the pursuit of a public task.
- **Task in the Public Interest**
  Processing is necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
- **Consent**
  We hold clear, specific, and unambiguous consent for the individual's data to be processed for a specific purpose.

1.2.3 The College will not process personal data unless it is carried out with the consent of the individual or is satisfied that processing conforms to one of the aforementioned legal bases.

### 1.3 Deciding which condition to rely on

1.3.1 If you are making an assessment of the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means.

1.3.2 Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

1.3.3 Consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

1.3.4 Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

1.3.5 We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

1.3.6 If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the DPO.

# 2. Responsibilities

### 2.1 Our Responsibilities

2.1.1 The College as a data controller has overall responsibility for compliance with data protection legislation. This can be broadly split into the six Principles.

2.1.2 GDPR contains a seventh principle, that of accountability, which states that the College is responsible for, and must be able to demonstrate, compliance with the principles.

2.1.3 To support compliance with the data protection legislation and this policy, the key responsibilities of the College are outlined below. This list is not exhaustive:

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual

- Identifying the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Storing data in safe and secure ways
- Assessing the risk that could be posed to individual rights and freedoms should data be compromised
- Ensuring all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and this policy.

2.1.4 Any breaches of the Data Protection Act 2018 by the College may lead to prosecution brought by the ICO. The ICO has the power to impose monetary penalties on the College of up to €10m or 2% of global turnover (whichever is higher) for breaches relating to 'standard' personal data. If the breach related to special category personal data, the monetary penalty maximums increase to €20m or 4% of global turnover (whichever is higher).

## 2.2 Your Responsibilities

2.2.1 Compliance with data protection legislation is the responsibility of all Governors and staff of the College. Any breach of data protection legislation, whether deliberate or caused by negligence, may lead to disciplinary action being taken in line with the College's disciplinary procedures.

2.2.2 Where it considers it necessary, the ICO has the power to bring legal proceedings against individuals who are responsible for breaches of the Data Protection Act 2018, in addition to the organisation by which they are employed. This may include senior staff who have knowingly allowed activities to take place in contravention of the Data Protection Act 2018, or staff who have wilfully acted against the law. Prosecution in these circumstances may lead to unlimited fines against the individual.

2.2.3 Line managers have responsibility to ensure that their staff have sufficient and up-to-date data protection training in line with the College's mandatory training requirements.

2.2.4 To support compliance with data protection legislation and this policy, the key responsibilities of each individual are outlined below. This list is not exhaustive:

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.

2.2.5 The College will always consider any suggestions to improve data handling and data procedures, and to that end encourages staff to be involved in the development of safe, secure and legal processing of personal data. Staff should feel free to suggest any actions that they feel would improve the procedures and/or security of the College's processing of personal data without fear of disciplinary action related to any such suggestions.

## 2.3 Responsibilities of the Data Protection Officer

2.3.1 As a public authority under data protection legislation, the College appoints a DPO with defined responsibilities.

2.3.2 To support compliance with data protection legislation and this policy, the key responsibilities of the DPO are outlined below. This list is not exhaustive:

- Keeping the Board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Providing data protection advice for all staff members
- Answering questions on data protection from staff, Board members and other stakeholders
- Responding to individuals who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the College's data any contracts or agreement regarding data processing
- Maintain a register of processing activities that the College undertakes
- Maintain a breach register and undertake any breach report investigations in line with the guidance in section 2.72.7 Data Security and Breach Reporting.

## 2.4 Accuracy and relevance

2.4.1 The College is responsible for ensuring 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.

2.4.2 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. For more information see 3.3 Right to rectification.

## 2.5 Retention

2.5.1 The College retains personal data for no longer than is necessary. In some cases, this is defined by law; in other cases, the College maintains its own retention guidelines. These will vary depending on the type and amount of personal data processed, the reasons for the processing and legal basis under which the processing took place.

2.5.2 The College retention schedule can be found on the College intranet and website[1].

## 2.6 Transfers of data

2.6.1 The College will only transfer data to another organisation where an appropriate contract and/or data sharing agreement is in place.

[1] http://www.wakefield.ac.uk/_downloads/policies-and-procedures/data-protection/Document%20Retention%20Schedule%20May%202018.docx

2.6.2 The College will only consider transferring data to another country where the receiving party is located in a country with adequate data protection provisions[2]; where the transfer is subject to the appropriate safeguards (including but not limited to standard contract clauses approved by the European Commission or compliance with an approved code of conduct approved by a supervisory authority); or where the College and the receiving party have signed Binding Corporate Rules.

## 2.7 Data Security and Breach Reporting

2.7.1 All staff are responsible for ensuring that personal data is kept secure against loss, misuse, or unlawful disclosure. Where other organisations process personal data as a service on the College's behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

2.7.2 Relevant, appropriate steps will be taken by all employees to prevent unlawful disclosure or loss of personal data. These include but are not limited to:

- Printed data should be kept securely where it cannot be accessed by unauthorised personnel.
- Printed data should be disposed of in confidential waste bins when no longer needed.
- Storage cabinets and rooms containing printed personal data will be locked when not in use, and their keys stored in lockable key safes.
- Personal data should not be disclosed in any form to any unauthorised third party. Identity checks must be carried out before disclosing student information to students or authorised student contacts. Disclosure of data to other organisations must be supported by a signed contract and/or data sharing agreement, or Schedule 2 part 1 of the Data Protection Act 2018.
- Data will be backed up regularly in line with the College's backup and security procedures.
- Removable media is not accessible from any staff computers with the exception of cases approved by the Head of IT Services and DPO.
- Staff computers in public areas will be fitted with privacy screens or placed in locations where their displays are not visible to the public.
- Where possible, students should not be granted access to staff offices where personal data processing is taking place. Where such access is necessary, students will never be unsupervised during this time.
- All possible technical measures must be put in place to keep data secure, including hardware encryption and user access control.

2.7.3 Any breach of data security must be reported to the DPO as soon as it is discovered. The DPO will decide whether a detailed investigation needs to be undertaken, whether the individuals concerned should be notified, whether any other organisations should be notified, and whether the breach needs to be reported to the ICO. Recommendations from any breach report investigation will cover changes to procedures and remedial action only.

2.7.4 Further details on breach reporting procedures can be found in section Data Breaches.

[2] For a list of countries with adequate data protection provisions, see https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

# 3. The Rights of Individuals

## 3.1 Right to be informed

3.1.1 Individuals have a right to be informed about the collection and use of their personal data. The College will provide all data subjects with information including the purposes for processing personal data, retention periods and who this data will be shared with, at the point of collection.

3.1.2 If the personal data is not received from the data subject, and the data subject does not already have this information, then they must be informed of this information within a reasonable timescale and no later than one month after receiving the data.

3.1.3 Further details about how to use privacy statements can be found in section Privacy Notices.

## 3.2 Right of access

3.2.1 Individuals have the right to access all the personal data that an organisation keeps on them.

3.2.2 Any individual can make a request, written or verbally, to any member of staff at the College. A request does not have to follow a formal process, therefore this includes telephone requests by a member of the public, or a verbal request in a meeting by an employee.

3.2.3 The College must provide this information to the data subject as soon as possible, and at the latest within one calendar month of the request being received (the time limit should be calculated from the day the request is received (whether it is a working day or not) until the corresponding calendar date in the next month). The data must be provided at no cost to the individual. Where possible, the data should be provided in a commonly used electronic format, especially if the request is made electronically, and securely transferred to the data subject.

## 3.3 Right to rectification

3.3.1 Data subjects have the right to have any personal data stored by an organisation rectified where it is incorrect, or to have incomplete information completed.

3.3.2 If any member of College staff receives a request to correct personal data because it is incorrect or incomplete, they must take reasonable steps to verify the accuracy of the updated information provided by the data subject. Greater care must be taken when correcting data that would have a significant impact on the College or individual (for example a date of birth that may affect funding eligibility) than minor information (for example a personal email address used for marketing purposes).

## 3.4 Right to erasure

3.4.1 Also known as the right to be forgotten, data subjects have the right to ask for their personal data to be erased in the following circumstances:

- the personal data is no longer necessary for the purpose which the College originally collected or processed it for;
- the College is relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;
- the College is relying on legitimate interests as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the College is processing the personal data for direct marketing purposes and the individual objects to that processing;
- the College has processed the personal data unlawfully;

- the College has to do it to comply with a legal obligation; or
- the College has processed the personal data to offer information society services to a child.

## 3.5 Right to restrict processing

3.5.1 As an alternative to requesting erasure, an individual has the right to request that the College restricts or entirely ceases processing their personal data.

3.5.2 This right only applies in the following circumstances:

- the data subject contests the accuracy of their personal data and the College is verifying the accuracy of the data;
- the data has been unlawfully processed and the data subject opposes erasure and requests restriction instead;
- the College no longer needs the personal data and would delete it under its retention policy, but the data subject requests the College keep it in order to establish, exercise or defend a legal claim; or
- the data subject has objected to you processing their data under their right to object, and the College is considering whether its legitimate grounds override those of the data subject.

3.5.3 Where a data subject exercises their Right to rectification or Right to object, they may also request that the College restricts processing while we consider their rectification or objection request.

## 3.6 Right to data portability

3.6.1 The right to data portability only applies to data that the individual has provided to College. It allows them to move, copy or transfer personal data from one system to another.

3.6.2 Data provided to the College includes data generated from their behaviour, such as attendance or web browsing history, but excludes data that the College has created based on the individual's actions, such as pastoral or behavioural comments.

3.6.3 The data subject has the right to receive a copy of their data, and/or to have their data transferred from one data controller to another where this is technically feasible. Where this occurs, it is essential that the data transfer is secure, and follows the same level of security as any other data transfer between organisations.

## 3.7 Right to object

3.7.1 Individuals have the right to object to their data being processed. When an individual exercises this right, the College will stop processing the data subject's data until it can establish whether the College has a compelling reason to resume processing.

3.7.2 Objections can be raised verbally or in writing and must be responded to within one month.

3.7.3 In cases where the objection relates to processing the data subject's data for the purposes of direct marketing, the College will respect the objection and will cease any marketing activities to the data subject.

## 3.8 Rights related to automated decision making

3.8.1 If the College undertakes any solely automated decision making and/or profiling then it will only ever do this under a contractual, legal, or consent basis.

3.8.2 The College will offer all individuals the opportunity to request human intervention or challenge any automated decision making.

# 4. Privacy Notices

## 4.1 When to supply a privacy notice

4.1.1 When the data is collected directly from the data subject, the privacy notice must be provided at the point of collection.

4.1.2 When the data is collected from a third party, the data subject must be provided with a privacy notice by the College within a reasonable period of obtaining the data (and not later than one month), and not after the first communication with the data subject takes place.

4.1.3 If the data subject has already been provided with an appropriate privacy notice when the data was collected, then the College does not need to provide further privacy information.

## 4.2 Contents of a privacy notice

4.2.1 All privacy notices that the College provides will contain:

- the identity and the contact details of the data controller (i.e. the College);
- the contact details of the DPO;
- the purposes the personal data will be used for as well as the legal basis for the processing;
- the legitimate interest will be specified, where legitimate interests is the legal basis for processing;
- the recipients/categories of recipients of the personal data, if any;
- details of data export and the safeguards applied;
- the period the personal data will be stored;
- the rights of the individual (see The Rights of Individuals);
- where the individual has given consent, the right to withdraw that consent;
- the right to lodge a complaint with the ICO;
- the existence of automated decision making including profiling, the logic involved, as well as the significance and envisaged consequences; and
- whether the provision of the data is a statutory or contractual obligation and of the possible consequences of failure to provide such data.

4.2.2 Where the data has not been collected directly from the data subject, the privacy notice provided by the College will also state the nature and scope of personal data being processed.

## 4.3 How to supply a privacy notice

4.3.1 The College takes a layered approach to the provision of privacy notices to data subjects.

4.3.2 Initial privacy statements will be included with any forms which collect new data from the data subject. These privacy statements will typically include reference to the data collected, the purpose of processing, and a link to further information provided online on the College Privacy Notice webpage. Examples of these privacy statements can be found in Appendix 2: Privacy Statement Examples.

4.3.3 The College will supply full privacy information as detailed in section 4.2 through online privacy notices.

4.3.4 If the College changes how it uses personal data, the College may need to notify data subjects about the change. If any College staff intend to change how they use personal data, they must notify the DPO who will decide whether the intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

# 5. Subject Access Requests

## 5.1 How we deal with subject access requests

5.1.1 Data subjects are entitled to ask for any data that the College holds on them and has generated about them. Some subject access requests are simple and straightforward (e.g., result checks and academic history requests) and should be completed under departmental procedures.

5.1.2 Some requests may comprise a significant amount of data, so good practice is to establish whether the data subject only wishes to receive a specific subset of data. For this purpose, a form is provided in Appendix 3: Subject Access Request form of this policy to establish what personal data is being requested.

5.1.3 Where the request is particularly complex, the deadline can be extended by up to a further two months, but the data subject must be informed that the College intends to do so, and why the extra time is needed.

5.1.4 Where the request is unfounded or excessive, in particular in cases where the request is repetitive (e.g., a second request for employment history after one such request has already been fulfilled), the College may charge a reasonable fee to provide this information, or refuse to respond to the request. In these circumstances, contact the DPO for further guidance.

5.1.5 For further detail regarding procedure and compliance with subject access requests, please contact the DPO.

# 6. Requests for erasure

## 6.1 How we deal with requests for erasure

6.1.1 When a data subject requests that their data be erased, The College will erase that data unless we need or have to keep it.

6.1.2 The College may decide that the data subject is unable to exercise their right to erasure if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

6.1.3 In many circumstances, the College processes data as a public task, and in these cases the right to erasure does not apply. Examples could include the processing of educational history, or of safeguarding records.

6.1.4 Where the data subject does have the right to erase their data, the college will comply with the request. The College will keep personal data of the individual requesting erasure only to the

extent that it can be used to show that the individual had their data erased and to ensure that the erasure was completed.

6.1.5 Where the data subject's data has already been disclosed to a third party (for example through a data sharing agreement), the College will tell any third party that has received a copy of the data that the data subject has exercised their right to be forgotten and they must too erase the data, unless this is impossible or would involve disproportionate effort.

6.1.6 For further detail regarding procedure and compliance with requests for erasure, please contact the DPO

# 7. Third parties

## 7.1 Using third party controllers and processors

7.1.1 As a data controller and data processor, the College must have written contracts in place with any third party data controllers and/or data processors that the College uses. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

7.1.2 When operating as a data controller, the College must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

7.1.3 When operating as a data processor, the College must only act on the documented instructions of a controller. The College will acknowledge its responsibilities as a data processor under GDPR and will protect and respect the rights of data subjects.

7.1.4 Where the College contracts any consultants that may have access to any personal data, they will be required to read this data protection policy and declare their understanding of their responsibilities using the form in Appendix 4: . This form should be submitted to the DPO once completed.

7.1.5 When the College employs any new members of staff, they will be required to read this data protection policy and declare their understanding of their responsibilities using the form in Appendix 4: if they will have any access to personal data before undertaking their data protection training. This form should be submitted to the DPO once completed.

## 7.2 Contracts

7.2.1 The College's contracts will comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. The College's contracts with data controllers and data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

7.2.2 At a minimum, all contracts that the College enters into that include the processing of personal data will include terms that specify:

- The data processor will act only on the written instructions of the data controller
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR

- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections and provide whatever information necessary for the data controller and data processor to meet their legal obligations.
- Nothing will be done by either the data controller or data processor to infringe on the GDPR or any relevant Data Protection Legislation.

7.2.3 The College has a defined procedure for contract drafting and approval, which includes provision for data protection. Following these instructions will ensure compliance with the data protection legislation including the Data Protection Act 2018 and GDPR. For further details on this procedure, contact the College's Legal Officer.

# 8. Data Breaches

## 8.1 Legal obligation to report breaches

8.1.1 Any breach or suspected breach of either this policy or data protection legislation by the College (or any member of its staff) should be raised with the DPO as soon as the College (or any member of its staff) becomes aware of the breach. The DPO will begin an investigation into the breach.

8.1.2 If the DPO considers the breach to be likely to result in a risk to the rights and freedoms of the data subjects whose personal data is involved in the breach, they will notify the ICO of the breach as soon as possible (and in any case not longer than 72 hours after the breach being identified).

8.1.3 If the DPO considers the breach to be likely to result in a high risk to the rights and freedoms of the data subjects whose personal data is involved in the breach, they will also inform the individuals themselves.

8.1.4 Reporting a breach allows the College to investigate any breaches and maintain a log of data breach incidents. This log allows for continual monitoring of compliance failures, and to identify points of weakness in policy and procedure.

# 9. Complaints against the DPO

## 9.1 How we deal with complaints against the DPO

9.1.1 Complaints relating to the conduct of the DPO should be made directly to the Vice Chair of Governors who shall be responsible for investigating the same.

9.1.2 Where the Vice Chair of Governors, having completed his/her investigations, considers a complaint to be valid, he/she shall take such actions as he/she considers necessary to address the matter including but not limited to taking disciplinary action against the DPO, retraining the DPO, relieving the DPO of his/her duties, taking steps to rectify the actions of the DPO and, where he/she considers that the actions of the DPO are likely to result in a high risk to the rights and freedoms of data subjects, reporting the actions of the DPO to the ICO.

9.1.3 Upon completion of the investigations set out in paragraph 9.1.2, the Vice Chair of Governors must communicate his findings including the actions to be taken (if any) to the complainant, as soon as possible.

9.1.4 If the complainant confirms that he/she is dissatisfied with the outcomes communicated by the Vice Chair of Governors, in accordance with paragraph 9.1.3, he/she will be entitled to complain directly to the Chair of Governors who shall investigate the matter. The Chair of Governors shall communicate his/her findings and any actions to be taken to the complainant as soon as possible.

9.1.5 If the complainant confirms that he/she is dissatisfied with the outcomes communicated by the Chair of Governors, in accordance with paragraph 9.1.4, he/she shall be asked to direct his/her complaint to the ICO, direct.

# 10. Audits, monitoring and training

## 10.1 Data audits

10.1.1 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.

10.1.2 The DPO is responsible for maintaining this list.

10.1.3 You are responsible for ensuring that any new data processing activities that you or your department undertake are reported to the DPO for inclusion in the register, and that any material changes to data processing activities (e.g. processing data for a different purpose) are approved by the DPO before they commence.

10.1.4 The register of processing activities is shared on the college intranet and is available on the Data Protection SharePoint site.

## 10.2 Monitoring

10.2.1 The DPO has overall responsibility for this policy, and the College's adherence to relevant data protection legislation.

10.2.2 The College will keep this policy under review and amend or change it as required.

## 10.3 Training

10.3.1 All staff are required to complete training on data protection within the first month of employment, and subsequently refresh this training every three years.

10.3.2 In instances where this policy has been breached, the DPO may mandate further training and/or refresher sessions on data protection compliance.

# Appendices

## Appendix 1: ICO Registration

| | |
|---|---|
| **Registration number:** | Z7613845 |
| **Date registered:** | 03 February 2022 |
| **Registration expires:** | 02 February 2023 |
| **Data controller:** | **the** College |
| **Address:** | Margaret Street<br>Wakefield<br>West Yorkshire<br>WF1 2DH |

Full details of the College's registration with the ICO can be found online at https://ico.org.uk/ESDWebPages/Entry/Z7613845

## Appendix 2: Privacy Statement Examples

Example 1

Heart of Yorkshire Education Group will use [details of personal data collected] in order to [purpose of data collection]. For further details on how we protect your personal data, see [insert link to College Privacy Notice].

Example 2 (specific retention period outside retention policy)

Heart of Yorkshire Education Group will use [details of personal data collected] in order to [purpose of data collection]. The data will be kept for [retention period] and then deleted/destroyed. For further details on how we protect your personal data, see [insert link to College Privacy Notice].

Example 3 (consent example)

Heart of Yorkshire Education Group will use [details of personal data collected] in order to [purpose of data collection]. We are doing this because you have consented above. If at any time you decide that you no longer consent to us processing your data for [purpose of data collection] then let us know and we'll stop. If you withdraw or withhold your consent, it will not affect your existing or any future relationship with the College. For further details on how we protect your personal data, see [insert link to College Privacy Notice].

## Appendix 3: Subject Access Request form

I, (print name) _____ wish to have access to the following personal data that the College processes relating to me:

| | |
|---|---|
| ☐ | Academic marks or course work details |
| ☐ | Academic or employment references |
| ☐ | Disciplinary records |
| ☐ | Health and medical matters |
| ☐ | Political, religious or trade union information |
| ☐ | Any statements of opinion about my abilities or performance |
| ☐ | Biographical details including name, address, date of birth etc. |
| ☐ | Other information (please specify): |

| |
|---|
| |

**OR**

| | |
|---|---|
| ☐ | All the data that the College currently has about me, either in a computerised system or appropriate paper-based filing system |

*While the College will comply with requests for access to personal data where the data protection legislation allows it, the College will be able to comply much more rapidly to specific requests rather than general requests. In any case, the College will return the information requested within one calendar month of receiving the request.*

*If for any reason the College is unable to comply by this deadline, for example the request is particularly complex, we will explain to you why we will not be able to return the requested data within the original deadline, and when we will be able to provide it.*

| | | | |
|---|---|---|---|
| Name | | | |
| Contact telephone/email | | | |
| Address | | | |
| Signed | | Date | |

Heart of Yorkshire Education Group will use the details provided on this form in order to contact you and provide the information requested. For further details on how we protect your personal data, see [insert link to College Privacy Notice].

## Appendix 4: Data Protection awareness declaration

Data protection legislation is concerned with personal information used in computer systems and other automated equipment, including CCTV. It also applies to some paper records. The main purpose of the legislation is to protect the individual's right to privacy and from being harmed by the misuse of personal information.

The legislation makes the College and its employees responsible for the fair processing, accuracy, relevance and security of personal data held on ALL computer and relevant filing systems within the College. Employees at any level could be liable to prosecution if any damage and associated distress is caused to an individual by the loss, destruction or unauthorised disclosure of personal data, or by the holding of inaccurate data.

### Your Duties as an Employee

You should ensure that you handle personal data according to the College's Data Protection Policy and, in particular, ensure that it:

- is obtained fairly and lawfully;
- is not entered onto a computer in ways which are not permitted by the College;
- is accurate, relevant and held for no longer than is necessary;
- is protected by proper security;
- cannot be read or seen by members of the public or anyone who should not see it;
- is not left on screen when leaving the office; and
- is not disclosed to external organisations or people, except in accordance with the College's Data Protection Policy.

The College's Data Protection Policy can be found on the college Intranet at the following link [please insert link to the Data Protection Policy.

By signing this form you declare that you have read the College's data protection policy, agree to abide by the contents, and operate in compliance with the data protection legislation.

| | |
|---|---|
| Name (print) | |
| Signature | |
| Employer | |
| Date | |

## Appendix 5: Key Contacts

| Staff | Job Title | Extension |
|---|---|---|
| Sam Cremore | Data Protection Officer | 3208 |
| Chris Holt | Head of Management Information | 3399 |
| Jason Pepper | Executive Director of Finance and Resources | 3206 |
| Mike Penty | Head of IT Services | 3212 |