

AWARD-WINNING EDUCATION

HOPWOOD HALL COLLEGE  
**Data Protection  
Policy**

**2024 - 2025**



## Policy Cover Sheet

Please fill in the following details:

Policy Name	Data Protection Policy
Version Number	V1.3
Policy Owner	Matthew Taylor
Release Date	
Policy valid for	1 year / 2 years / 3 years

Documents included:

Completed Checklist (below)	X
Policy text	X
Filled in EIA	X

Where should this policy be shared? All policies will be shared on the HUB.

The HUB	X
Net Consent	
Website	

### Policy Checklist

Have you completed the following tasks:

Used the Microsoft Accessibility Checker	X
Used formatted headings	X
Used Arial 12pt font	X
Included numbered paragraphs	X
Included page numbers	X
Included alternative text for all images which accurately describe what's in the picture	N/A
Checked for gender neutral language e.g. remove dinner ladies, workmen, he/she and replaced with servers, contractors, they.	X
Used the full phrase instead of the acronym at least the first time	X
Used the spelling and grammar check	X
Gained feedback from colleagues to ensure the policy is clear and accurate	X
Included any legal, social or organisational changes since the last policy review	X
Reviewed the connected policies to ensure they are still active	X
Filled in the change log	X
Listened to the policy using the accessible reader	X
Reviewed the policy flowchart	X
Informed the EDI Manager of upcoming policy deadlines	

**Sign Off: To be filled in by the named person only**

	Name	Date
SLT		
Corporation (if required)		
Trade Union		
EIA		

## Change log

Version number	Changes description	Major changes? Y/N	Initiator	Rationale	Date of completion	New version number
V1.0	Updates to the policy	N	Matthew Taylor		01/11/2024	V1.1
V1.1	Updated formatting	N	Matthew Taylor		05/11/2024	V1.2
V1.2	Updated formatting and content	N	Matthew Taylor		29/01/2025	V1.3

## CONTENTS

1. INTRODUCTION .....	4
2. SCOPE .....	4
3. AIM .....	4
4. ROLES AND RESPONSIBILITIES .....	4
5. PROCEDURE.....	8
7. DOCUMENTS ASSOCIATED WITH THIS POLICY .....	22
8. APPENDIX .....	22

## 1. INTRODUCTION

- 1.1. Hopwood Hall College is committed to ensuring that all personal data collected is processed in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other related legislation.
- 1.2. Hopwood Hall College is registered as a Data Controller with the Information Commissioners Office (ICO) under Registration Number **Z6764170**
- 1.3. If you have any queries concerning this Policy, please contact our Data Protection Officer at [DPO@Hopwood.ac.uk](mailto:DPO@Hopwood.ac.uk)
- 1.1. Definitions for terms used in this policy can be found in the [Appendix 3](#)

## 2. SCOPE

- 2.1. This policy applies to staff, students and all key stakeholders at Hopwood Hall College including governors, volunteers, parents/carers, visitors, contractors, and other community users. Compliance with the Act is the responsibility of all members of Hopwood Hall College. Any deliberate breach of the data protection policy may lead to disciplinary action.

## 3. AIM

- 3.1. This Policy (and the other associated policies and documents referred to in it) sets out the basis on which the College will collect and use Personal Data either where the College collects it from directly from individuals, or where it is provided to the College by third parties. It also sets out the rules on how the College handles uses, transfers, and stores Personal Data.
- 3.2. This policy does not form part of any College's employee's contract of employment, but all members of staff are expected to comply with this and related policies at all times. Any failure to follow the policy can therefore result in disciplinary proceedings.

## 4. ROLES AND RESPONSIBILITIES

### 4.1. All College Personnel:

- 4.1.1. Must comply with this policy as well as associated policies and documentation, including the College's IT policies in relation to security, as outlined in paragraph 14 (Related Policies) [Insert link to paragraph 14].

4.1.2. Must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

4.1.3. Must not release or disclose any Personal Data:

- Outside the College; or
- Inside the college to College Personnel not authorised to access the Personal Data,
- Without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

4.1.4. Must take all steps to ensure there is no unauthorised access to Personal Data whether by other College Personnel who are not authorised to see such Personal Data or by people outside the College.

4.1.5. Must ensure they discuss any proposed new uses of personal data with the Data Protection Officer (DPO).

4.1.6. Must ensure that personal data is destroyed in accordance with the College's [Data Retention Policy](#)

4.1.7. Are responsible for undertaking data protection and information handling training as directed.

4.1.8. Must ensure that all information they provide to the College in relation to their employment is accurate and up to date. They must inform the College of any changes to the information they have provided.

## **4.2. Student Responsibilities**

4.2.1. Students must ensure that all information they provide to the College in connection with their enrolment is accurate and up-to-date. They must inform the College of any changes to the information they have provided, for example change of address, emergency contact details. This will enable the College to update its Management Information System.

4.2.2. Students must not seek to gain unauthorised access to personal information.

4.2.3. Students must comply with all [College policies](#) regarding the use of IT facilities.

### **4.3. Management Responsibilities**

4.3.1. Managers are responsible for:

4.3.2. Ensuring the lawful processing of personal data within their department or area of responsibility.

4.3.3. Managers are responsible for liaising with the Data Protection Officer in relation to keeping the College's Record of Processing Activity up to date with regard to processing within their department or area of responsibility.

4.3.4. Managers must ensure that the processing of personal data complies with all appropriate College policies.

4.3.5. Managers must ensure that personal data is destroyed in accordance with the College's Data Retention Policy.

4.3.6. Managers must ensure that all data subject rights requests received in writing or verbally are passed to the Data Protection Officer within 48 hours of receipt.

### **4.4. IT and Management Information Systems (MIS) Staff Responsibilities**

4.4.1. Whilst all staff and users of personal data have responsibility for the security of data, IT and MIS staff have an important role in ensuring the security of computerised data. In particular, IT and MIS:

4.4.2. Are responsible for advising the College on the state of technological development with regard to IT security.

4.4.3. Are responsible for providing secure methods of transferring authorised personal data outside the College.

4.4.4. Ensure that data is backed up on the College's IT systems and maintain appropriate disaster recovery procedures.

4.4.5. Implement virus detection and hacking preventative measures.

- 4.4.6. IT and MIS ensure, through liaison with appropriate College personnel, that the College's business systems are secure and appropriate restrictions on access are in place so that individuals only have access to personal data in which they have a legitimate business interest.
- 4.4.7. Are responsible for reviewing and updating College IT policies in relation to the use of IT systems including email, the internet and intranet.
- 4.4.8. Investigate breaches of IT security as well as near misses, working with the Data Protection Officer to ensure that data breaches are investigated and reported as necessary in compliance with data protection legislation.
- 4.4.9. Ensure that data is deleted according to the College's [Data Retention Policy](#)

#### **4.5. Data Protection Officer (DPO)**

- 4.5.1. The Data Protection Officer is responsible for:
- 4.5.2. Advising on the implementation of this and related policies.
- 4.5.3. Keeping information law policies and procedures under review and developing policies and guidance as required.
- 4.5.4. Monitoring compliance with this and related policies, ensuring College data processing complies with data protection law.
- 4.5.5. Providing advice and guidance on data protection including data protection impact assessments and wider information law matters
- 4.5.6. Investigating personal data breaches and notifying the ICO and data subjects as necessary.
- 4.5.7. Responding to data subject rights requests (as well as requests under the Freedom of Information Act 2000 and the Environmental Information Regulations 2004) within statutory time frames and maintaining compliance logs.
- 4.5.8. Maintaining the College's registration with the ICO and acting as point of contact with the ICO as necessary.

4.5.9. Raising data protection awareness and ensuring data protection training requirements are complied with.

#### **4.6. Human Resources Responsibilities**

4.6.1. Human Resources will:

4.6.2. Ensure that Data Protection obligations are reflected in the College's Disciplinary Procedures and contracts of employment.

4.6.3. Ensure that all staff are aware of the types of personal information that the College will process on them and ask staff to check this information as required.

4.6.4. Ensure that all obligations outlined within the DBS Code of Practice are adhered to.

4.6.5. Provide advice to managers and others on the application of the DBS Code of Practice.

4.6.6. Destroy personal data according to the College's data retention policy.

## **5. PROCEDURE**

### **5.1. Data Protection Principles**

5.1.1. Data Protection Law requires the College to comply with the following principles. These principles require Personal Data to be:

5.1.2. **Processed lawfully, fairly and in a transparent manner.** The College maintains up to date privacy notices to ensure individuals are fully informed about what personal data is being processed and why. Where Personal Data is received about an individual from other sources, the College will provide the Individual with a privacy notice about how the College will use their Personal Data as soon as reasonably possible and in any event within one month.

The College identifies an appropriate lawful basis for processing Personal Data as well as additional conditions to justify the processing of special category and criminal offence data due to its sensitivity. As part of this the

College maintains an up to date Appropriate Policy Document which is kept under regular review.

**5.1.3. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.** The College ensures individuals are fully informed of the purpose of processing and records those purposes in privacy notices as well as wider documentation for accountability purposes. Should the purpose for which data is processed change over time or a new purpose arise, the College will only proceed if the new purpose is compatible with the original purpose, the individual consents to the new purpose or a clear legal provision requires or allows the new processing in the public interest.

**5.1.4. Adequate, relevant and limited to what is necessary for the purposes for which it is being processed.** The College ensures it only collects data that is actually needed for its specified purposes. We periodically review data and delete any data that is not needed to fulfil those purposes.

**5.1.5. Accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible.** The College ensures that data is recorded accurately and also records the source of the data provided. The College takes reasonable steps, having regard to the circumstances, the nature of the personal data and the purpose of processing, to ensure the accuracy of information.

The College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection legislation. The College has processes in place to respond to data subject rights requests appropriately and within statutory timescales.

**5.1.6. Kept for no longer than is necessary for the purposes for which it is being processed.** The College maintains a [Data Retention Schedule](#) that sets out how long all data, including special category data, shall be retained for. This Schedule is kept under regular review. The College also

reviews the data it holds at appropriate intervals as part of its regular review of the Record of Processing Activity held. When data held is no longer needed for the purpose it was collected for, the College ensures it is deleted or anonymised.

**5.1.7. Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.** The College has implemented appropriate technical measures to ensure the security of data processed. The College keeps its Information Security Policy, as well as IT Acceptable Use Policy, Risk Register, Disaster Recovery Plan, and IT Password Policy under regular review. The College ensures all staff undertake data protection training with annual refresher training.

5.1.8. In addition to complying with the above requirements the College also has to demonstrate in writing that it complies with them as part of its accountability obligations. The College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance. As part of this, we have an Appropriate Policy Document in relation to our processing of Special Category and Criminal Offence Data and we keep our Record of Processing Activity under regular review. The College also ensures that Data Protection Impact Assessments are carried out for processing likely to result in a high risk to individuals' interests.

## **5.2. Lawful Use of Personal Data**

5.2.1. Processing personal data will not be lawful without a valid lawful basis. Documenting our processing activities and the lawful basis on which the processing is justified is also a key part of our accountability obligation under the legislation.

5.2.2. To ensure that our processing of personal data is lawful, the College has carefully assessed how it uses personal data and has identified one of the six grounds set out in Article 6 of the UK GDPR as a valid basis on which to

process the data before the processing begins. Further information on the lawful bases can be found [here](#).

5.2.3. Where the College processes special category or criminal offence data, it has to show that one of a number of additional conditions is met. These are set out in Article 9 of the UK GDPR. These additional conditions have also been assessed and the College has identified which are applicable in order to justify its processing of special category or criminal offence data. Further information on the additional conditions for processing special category data can be found [here](#).

5.2.4. Determining the correct legal basis for processing data can be difficult and more than one ground may be applicable. Please contact the Data Protection Officer at [DPO@hopwood.ac.uk](mailto:DPO@hopwood.ac.uk) for advice and guidance.

5.2.5. The College records all processing activities and the way in which it meets its compliance obligations. If the College changes how it uses personal data, the record will be updated and individuals be notified of the change as necessary. As such, if College personnel intend to change how they use personal data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other measures which need to be taken.

### **5.3. Data Security**

5.3.1. The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Please see the following documents for further detail on this:

- [IT Security Policy](#)
- [IT Acceptable Use Policy](#)
- [IT Password Policy](#)
- e-Safety Guidelines (Available on ItsLearning)

- Disaster Recovery Plan (Available on College Intranet)
- Risk Register (Available on College Intranet)

## 5.4. Data Breaches

5.4.1. Whilst the College takes information security very seriously, unfortunately it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. In such an event, College staff must comply with the College's IT Personal Data Breach Reporting Policy (Available on College Intranet). This sets out important obligations in the event of a personal data breach and so all staff must ensure they are familiar with it to enable them to spot a breach or a near miss and to know what to do should such an event occur.

5.4.2. A Personal Data breach is defined as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.' Personal Data breaches can happen as a result of action taken by a third party, but they often occur as a result of something someone internal does, such as emailing personal data to the wrong person. Personal Data breaches can be deliberate or accidental.

5.4.3. There are three main types of Personal Data breach which are as follows:

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a College Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;
- **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data

stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

- **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

5.4.4. The College ensures that all college staff who have access to Personal Data are appropriately trained in data protection according to their role in order to reduce the likelihood of personal data misuse. This also ensures that staff are able to quickly recognise if a personal data breach has occurred to that swift action can be taken to mitigate the risks to data subjects and ensure compliance with the College's obligations in relation to data breaches.

## **5.5. Appointing Contractors who access the College's Personal Data**

5.5.1. Under Data Protection legislation, the College may only appoint a contractor to process personal data on behalf of the College where the College has carried out sufficient due diligence and only where there are appropriate written contracts in place.

5.5.2. A Data Controller is considered as having appointed a Data Processor where it engages a third party to perform a service on its behalf, as part of which they will require or obtain access to that Controller's Personal Data. Where the College appoints a Data Processor in this way, it is the College which remains responsible for what happens to its personal data.

5.5.3. The legislation requires that a Data Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals, which means that due diligence must be undertaken on both new and existing suppliers in relation to data protection requirements. Periodic audits must be carried out on Data Processors once appointed to ensure they continue to meet contractual requirements in relation to data protection.

5.5.4. The GDPR requires the contract with a Data Processor to contain the following obligations as a minimum:

- to only act on the written instructions of the Controller;

- to not export Personal Data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- to keep the Personal Data secure and assist the Controller to do so;
- to assist with the notification of Data Breaches and Data Protection Impact Assessments;
- to assist with subject access/individuals' rights requests;
- to delete/return all Personal Data as requested at the end of the contract;
- submit to audits and provide information about the processing and to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

5.5.5. In addition, the contract should set out:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of Personal Data and categories of individuals;
- and the obligations and rights of the Controller.

5.5.6. Any questions in relation to the College's use of Data Processors should be directed at the DPO at [DPO@hopwood.ac.uk](mailto:DPO@hopwood.ac.uk)

## **5.6. Individuals' Rights**

5.6.1. Data protection law gives individuals greater control over their personal data through several rights which the College strives to facilitate effectively.

5.6.2. Requests can be made verbally or in writing to [DPO@hopwood.ac.uk](mailto:DPO@hopwood.ac.uk)

5.6.3. As a member of College staff, if you receive a data subject rights request you should forward it to the DPO immediately and no later than within 24 hours of receipt. If the request is made verbally, please obtain as much information as possible, including contact details for the data subject, and pass them immediately to the DPO.

- 5.6.4. The College must respond to data subject requests within one calendar month. It is possible to extend the time to respond by a further two months if the request is complex or if we have received a number of requests from the individual. The College will let the individual know that the time limit needs to be extended within one month of receiving the request and will explain the reasons for the extension.
- 5.6.5. Generally there is no fee for making a data subject rights request, however the College may charge a reasonable fee for the administrative costs of complying with a request if it is manifestly unfounded or excessive. Where the College charges a fee, we will contact the individual promptly to inform them. Please note that the College does not have to comply with the request until we have received the fee.
- 5.6.6. Some rights only apply in certain circumstances, depending on the lawful basis for processing. The College may refuse to comply with a request if an exemption applies or if a request is manifestly unfounded or excessive. Every request will be dealt with on a case by case basis.
- 5.6.7. If an individual has a complaint about the way in which their data subject right request has been dealt with they should contact the Data Protection Officer at [DPO@hopwood.ac.uk](mailto:DPO@hopwood.ac.uk)
- 5.6.8. If an individual remains dissatisfied they have the right to complain to the Information Commissioner's Office [www.ico.org.uk](http://www.ico.org.uk)
- 5.6.9. Please contact the Data Protection Officer at [DPO@hopwood.ac.uk](mailto:DPO@hopwood.ac.uk) if you wish to withdraw consent to processing.
- 5.6.10. The procedure to be followed with regard to handling Subject Access Requests can be found at Appendix 1. The procedure to be followed when handling all other data subject rights requests can be found at Appendix 2.

## **5.7. Keeping Data Subjects Informed – Privacy Information**

- 5.7.1. Where the College collects personal data directly from individuals, the College will inform them about the nature and purpose of the processing in a

privacy notice published on the College's website. The full list of privacy information we must provide can be found

- [Privacy-Notice-for-Staff](#)
- [Privacy-Notice-for-Students](#)

5.7.2. Where personal data is collected directly from the individual, this information will be provided at the time of collection. Where we obtain personal data from another source we will, subject to exemptions, communicate this information, as well as the source and the categories of personal data processed, at the time of the first communication with the individual, or before personal data is disclosed to another party or in any event not more than one month after obtaining the personal data.

## **5.8. The Right of Access**

5.8.1. An individual may appoint another person to act on their behalf in requesting access to the information that the College holds about them. This is known as making a subject access request (SAR). When this happens, we will need written evidence that the individual concerned has authorised a third party to make the application and may also require further identification for the person making the request so we can be confident of their identity.

5.8.2. When an individual makes a subject access request, the data protection officer will tell them:

- Whether or not their data is processed and if so, why, the categories of personal data concerned and the source of the data if it is not collected from the individual.
- To whom their data is or may be disclosed, including to recipients located outside the European Economic Area and the safeguards that apply to such transfers.
- For how long their personal data is stored.
- Their rights to rectification or erasure of data, or to restrict or object to processing.
- Their right to complain to the Information Commissioner if they think the college has failed to comply with their data protection rights, and

- Whether or not the college carried out automated decision-making and the logic involved in any such decision-making.

5.8.3. The college will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

## **5.9. Right to rectification**

5.9.1. Individuals have the right to have inaccurate personal data rectified or, depending on the purposes for processing, to have incomplete data completed. On receiving a request for rectification, the College will take reasonable steps to determine the accuracy of the data we hold and will restrict processing the personal data in question while we do this. Further information can be found here [Right to rectification | ICO](#)

## **5.10. Right to Erasure**

5.10.1. The right to have personal data erased is also known as the 'right to be forgotten'. This applies only to data the College holds at the time the request is made, and not to data that may be created in the future. The right is not absolute and only applies in certain circumstances. Further information can be found here [Right to erasure | ICO](#)

## **5.11. Right to Restrict Processing**

5.11.1. As an alternative to the right to erasure, an individual can request that the way an organisation uses their personal data is limited. This is not an absolute right and applies in certain circumstances. Further information can be found here [Right to restrict processing | ICO](#)

## **5.12. Right to Data Portability**

5.12.1. Individuals have the right to request personal data they have provided to a controller in a structured, commonly used and machine-readable format. Individuals can receive their data and store it for future re-use or can request that a controller transmits this data directly to another controller. The right to data portability only applies in certain circumstances. Further information can be found here [Right to data portability | ICO](#)

### **5.13. Right to Object**

5.13.1. Individuals have the right to stop or prevent processing of their personal data. Whether the right to object applies depends on the purpose for the data is processed and the lawful basis for processing.

5.13.2. The right to object to processing of personal data for the purposes of direct marketing is an absolute right. Therefore when the College receives such a request it will suppress the personal data of the individual concerned retaining just enough to ensure that they do not receive direct marketing in future. Further information on the right to object can be found here [Right to object | ICO](#)

### **5.14. Rights related to Automated Decision Making including Profiling**

5.14.1. The College will not use personal data for the purposes of automated decision making that has legal or significantly similar effects on the individual unless the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by UK law; or
- based on the individual's explicit consent.

5.14.2. Where the College does use personal data in this way, individuals have the right to challenge such decisions, request human intervention in the process, express their own point of view and obtain an explanation from the College.

5.14.3. Where the College does use automated decision making, including profiling, we will:

- provide meaningful information about the way the decision-making process works, as well as explaining the significance and the envisaged consequences for the individual;
- use appropriate mathematical or statistical procedures;
- ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it;

- put appropriate technical and organisational measures in place, so that we can correct inaccuracies and minimise the risk of errors; and
- secure personal data in a way that prevents discriminatory effects and is proportionate to the risks to the individual's rights and interests.

## 5.15. Marketing and Consent

5.15.1. The College will only send direct marketing to individuals where they have given their explicit consent to receive such communications from us. Where the College carries out any such marketing, it ensures that it does so in a manner compliant with both Data Protection legislation as well as with the Privacy and Electronic Communications Regulations (PECR).

5.15.2. Individuals have the right to withdraw their consent at any time. To do so please contact Student and College Services at [administraton@hopwood.ac.uk](mailto:administraton@hopwood.ac.uk)

## 5.16. Automated Decision Making and Profiling

5.16.1. Under Data Protection legislation there are controls around profiling and automated decision making in relation to Individuals.

- **Automated Decision Making** happens where the College makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and
- **Profiling** happens where the College automatically uses Personal Data evaluate certain things about an Individual.

5.16.2. The College does not carry out Automated Decision Making or Profiling in relation to its students or its employees.

5.16.3. College Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer in order to ensure that the college is compliant with data protection legislation.

## 5.17. Data Protection by Design and Default and DPIAs

The concept of data protection by design seeks to ensure consideration of data protection issues at the outset and through the lifecycle of all processing activities. Data protection by default requires organisations to ensure that they

only process the data that is necessary to achieve the specific purpose in hand. It links to the fundamental data protection principles of [data minimisation and purpose limitation](#).

## **5.18. Data Protection Impact Assessments (DPIAs)**

5.18.1. DPIAs are a fundamental part of the concept of data protection by design in assessing the technical and organisational measures needed to ensure that processing complies with the data protection principles. DPIAs are also a key part of the accountability obligations under the GDPR.

5.18.2. A DPIA is not a prohibition on using personal data but is an assessment of issues affecting personal data which need to be considered before a new product or initiative is rolled out.

5.18.3. As such a DPIA should be started as early as practical in the design of processing operations so that College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

5.18.4. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- evaluate the risks to the rights and freedoms of individuals; and
- consider the measures required to address the risks identified.

5.18.5. All DPIAs must be reviewed and approved by the Data Protection Officer. Where a DPIA reveals a high risk which cannot be appropriately mitigated, the ICO must be consulted.

5.18.6. A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. Alongside this trigger, there are certain specific circumstances in which a DPIA is mandatory, namely the following:

5.18.7. Under the GDPR a DPIA must be completed if you plan to:

- Use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

5.18.8. The ICO also requires completion of a DPIA if you plan to:

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

5.18.9. It is important to note that consideration of data protection issues and risks is not just for new projects but may need to be addressed in relation to existing processing if the risks are sufficiently high and/or the way an activity is being carried out has changed. If you are unsure whether a DPIA is needed or have any questions about the process, please contact the DPO at [DPO@hopwood.ac.uk](mailto:DPO@hopwood.ac.uk)

5.18.10. The College uses the ICO's DPIA template which is available [here](#)

## **5.19. Transferring Personal Data to a Country outside of the EEA**

5.19.1. Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data

outside the EEA but also includes storage of Personal Data or access to it outside the EEA. This must be considered whenever the College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

5.19.2. In order to ensure that the College is compliant with Data Protection legislation, College personnel must not export Personal Data unless it has been approved by the Data Protection Officer.

## 6. MONITORING AND EVALUATION

6.1. This policy will be monitored and updated when changes are made to the ICO's guidelines.

## 7. DOCUMENTS ASSOCIATED WITH THIS POLICY

7.1. [Privacy Statement](#)

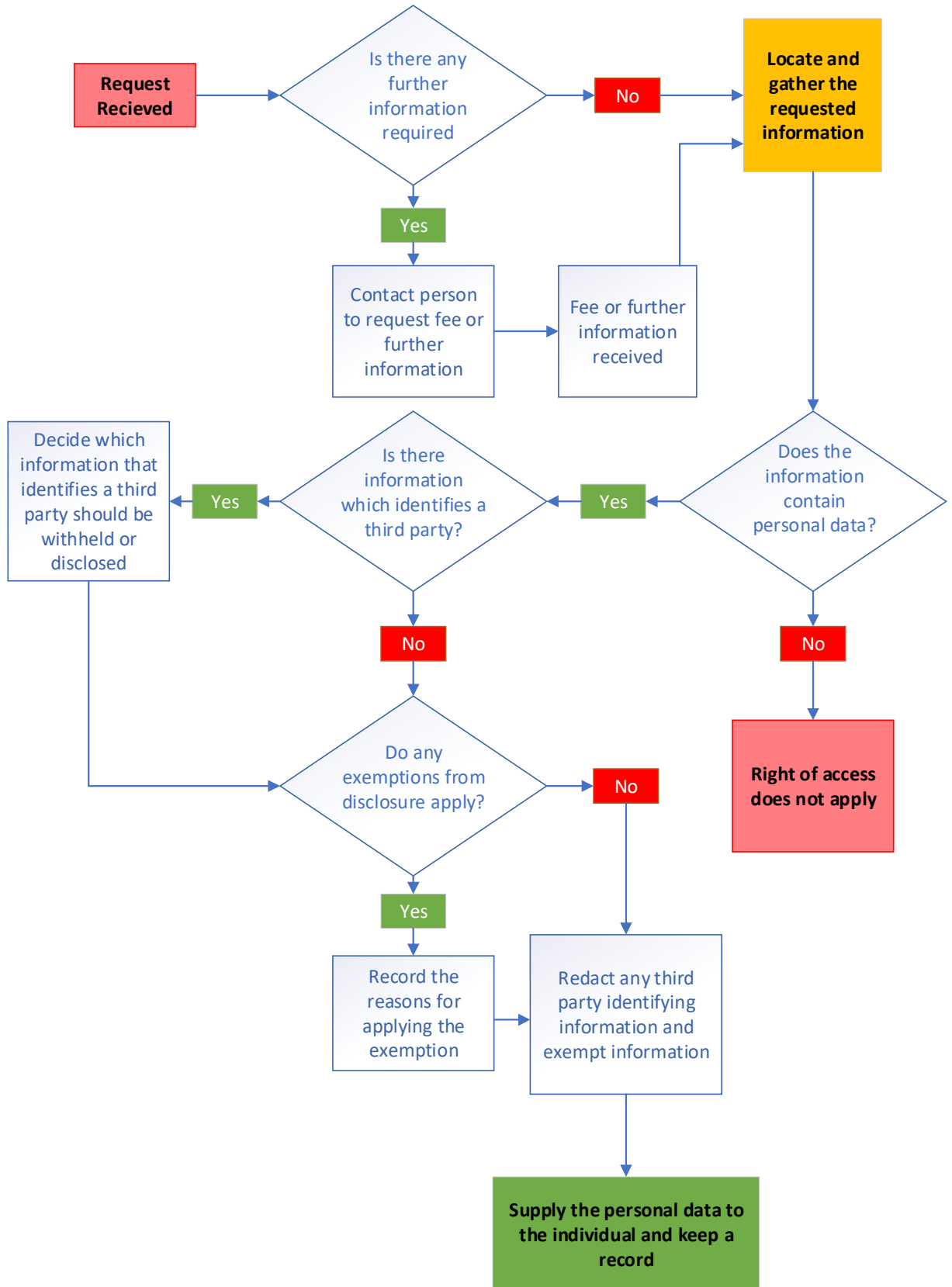
7.2. [Privacy Notice for Staff](#)

7.3. [Privacy Notice for Students](#)

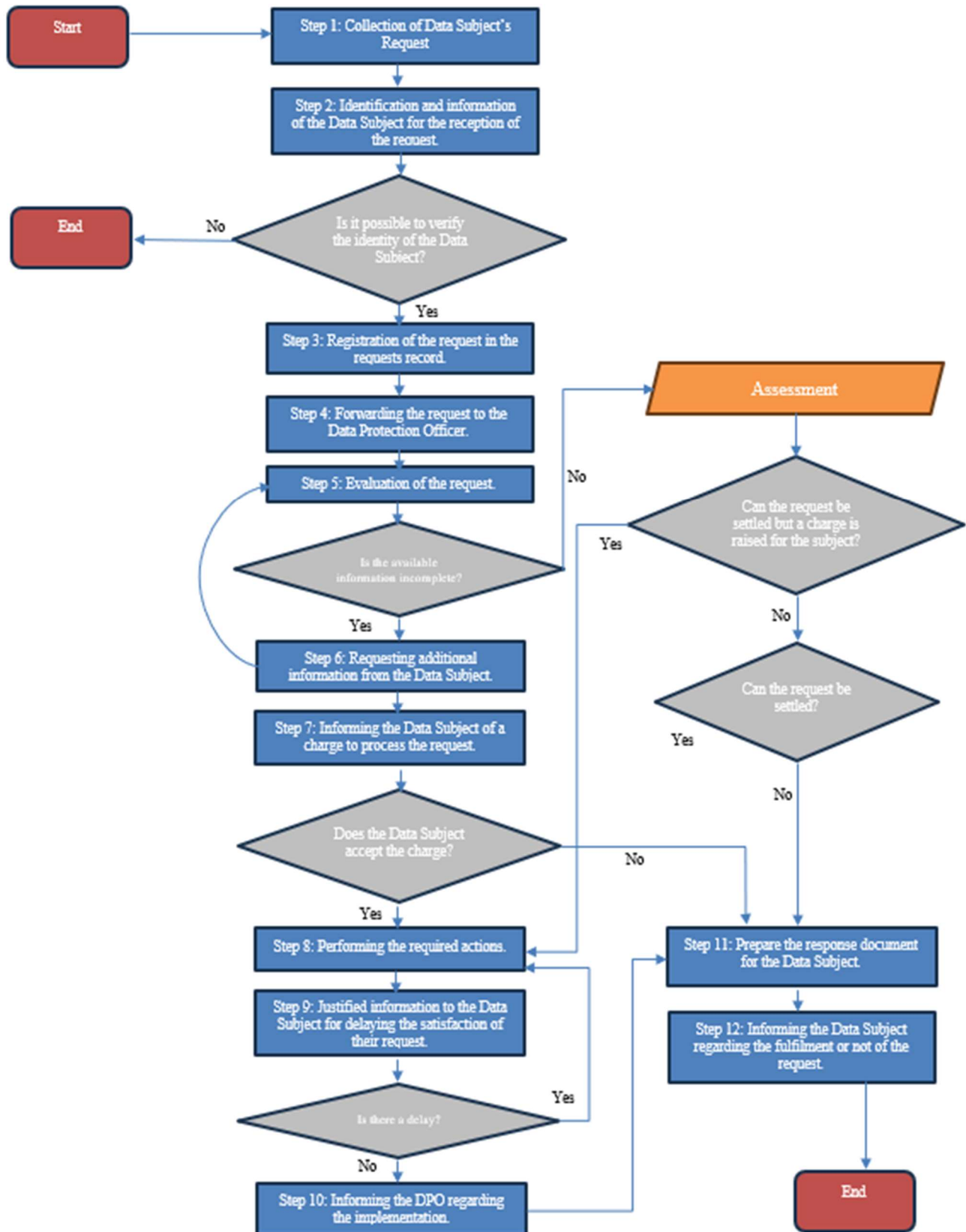
7.4. [Data Retention Policy](#)

## 8. APPENDIX

## 8.1. Appendix 1 – Subject Access Request Procedure



## 8.2. Appendix 2 – Procedure for handling other data subjects rights requests



## 8.3. Appendix 3 – Definitions

8.4. **College** – Hopwood Hall College and University Centre, Middleton Campus, Rochdale Road, Middleton, Manchester, M24 6XH and Rochdale Campus, St Mary's Gate, Rochdale, OL2 6RY.

8.5. **College Personnel** – Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

8.6. **Data Controller** – Any entity (for example company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.

8.6.1. A Data Controller is responsible for compliance with Data Protection Laws.

Examples of Personal Data the College is the Data Controller of include employee details or information the College collects relating to students. The College will be viewed as a Data Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it.

8.6.2. A common misconception is that individuals within organisations are the Data Controllers. This is not the case it is the organisation itself which is the Data Controller.

8.7. **Data Processor** – Any entity (for example company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller.

8.7.1. A Data Processor is a third party that processes Personal Data on behalf of a Data Controller. This is usually as a result of the outsourcing of a service by the Data Controller or the provision of services by the Data Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

8.8. **Data Protection Laws** – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

- 8.9. **Data Protection Officer** – Our Data Protection Officer is Ross Black, Student and College Services Manager. He can be contacted at [DPO@hopwood.ac.uk](mailto:DPO@hopwood.ac.uk)
- 8.10. **EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.
- 8.11. **ICO** – the Information Commissioner’s Office, the UK’s data protection regulator [Information Commissioner's Office \(ICO\)](#)
- 8.12. **Individuals** – Living individuals who can be identified, directly or indirectly, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors, and potential students. Individuals also include partnerships and sole traders.
- 8.13. **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.
- 8.13.1. Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as [firstname.surname@organisation.com](#)), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called ‘Special Categories of Personal Data’ and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

8.14. **Processing** - In relation to personal data, processing means any operation or set of operations which is performed on personal data or on sets of personal data such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction.

8.15. **Special Categories of Personal Data** – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data. Please note that criminal offence data is also subject to additional controls.

## Policy Guidance

### Timeline

Steps	Working Days	
<i>60 day reminder</i>		
(Re)Write policy	20	20
SLT sign off	10	30
<i>30 day reminder</i>		
Corporation sign off (if required)	Up to 90	
Trade Union sign off	5	35
Equality Impact Assessment	10	45
<i>14 day reminder</i>		
Final adjustments by Quality	3	48
Policy active on all platforms	1	49

These timings are approximate and are intended to be a guideline. If your policy needs Corporation Board sign off please contact the Clerk to the Corporation Fatema Hussein for dates to submit your policy to the board for discussion.

## Changes for 22/23

Change log: this has been added to the template. Below is an example change log:

Version number	Changes description and page number	Major changes? Y/N	Initiator	Rationale	Date active from	New version number
N/A	Major revisions, throughout	Y	Nicole Harding	Legal changes	23/5/22	V1
V1	Job title on page 6, section 3.12 updated from "Learning Support Officer" to "Learning Support Manager"	N	Nicole Harding	Department job roles change needed to be reflected in policy	31/9/22	V1.1
V1.1	Process revisions throughout	Y	Nicole Harding	Organisational processes changed upon annual review	23/5/23	V2

Details are given on what has changed, where, when, why, and by whom. This ensures we have appropriate version control, supports staff to read updated versions of policies, and provides an auditable trail.

### **Version numbers**

Per the example change log above, version numbers are updated upon every change. Minor changes means that the number after the decimal point changes, major changes means that the first number changes.

### **Paragraph numbering**

Paragraph numbering helps to track where changes are and make the document more accessible to those using screen readers. Microsoft will create this for you, and it is included on the template.

### **Slimming down policies and number of policies**

For 24/25 please consider whether all policies in your name are required; if any policies can be combined or if they are no longer relevant. Please also consider whether the contents of the policies are succinct and concise or if the size of the policies could be reduced.

# Policy Flowchart

## Policy Process 2022/2023

