Data Protection Policy

Responsible Senior Manager:	Deputy Principal Finance & Facilities
Effective Date:	May 2021
Related Policies:	General Use of Computer Equipment & Data Network Policy Freedom of Information Publication Scheme Public Interest Disclosure (Whistleblowing) Procedure Safeguarding Policy Disciplinary Policy
Approved By:	F&E Committee *
Next Review Date:	May 2024

* Under Delegated Powers

European Union
European Social Fund
Investing in jobs and skills

Contents

1. INTRODUCTION

Havant and South Downs College's (HSDC) reputation and future growth are, in part, dependent on the way that it manages and protects Personal Data. Protecting the confidentiality, integrity and availability of Personal Data is a key responsibility of everyone within the College.

HSDC collects, uses, and stores Personal Data about its employees, suppliers (sole traders, partnerships, or individuals within companies), students, governors, parents and visitors; the College recognises that having controls around the collection, use, retention and destruction of Personal Data is essential.

The College has implemented this Data Protection Policy so that all College staff know what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and provide a thriving working and learning environments for all.

College staff have access to this policy, along with other related policies on the College's Intranet. All staff are made aware of the contents of this policy when they start, and they are also advised of any revisions to the policy when they occur. Whilst, this policy is not part of the staff contract of employment and the College reserves the right to change the policy at any time and all members of staff obliged to comply with it at all times.

If you have any queries concerning this policy, please contact our Data Protection Officer, responsible for ensuring the College's compliance with this policy.

The Havant & South Downs College Corporation has agreed to adopt the Association of College's model.

2. ABOUT THIS POLICY

This policy (and the other policies and documents referred to in it) ensures the College complies with its obligations under data protection legislation. Personal data must be handled in line with the requirements of all data protection laws that protect the fundamental rights and freedoms of individuals.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

3. DEFINITIONS

3.1. **College** – HSDC (which comprises campuses at Havant, South Downs and Alton).

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

3.3. **Controller** – Any entity (e.g. company, organisation or person) determines the purposes and means of personal processing data.

3.4. **Data Protection Laws** – The UK GDPR (United Kingdom General Data Protection Regulation and all applicable laws relating to the collection and use of Personal Data and privacy and any relevant codes of practice issued by a regulator included in the UK, the Data Protection Act 2018.

3.5. **Data Protection Officer-** The Data Protection Officer (DPO) monitors internal compliance, informs, and advises on the college's data protection obligations and act as a contact point for data subjects and the Information Commissioner's Office (ICO). They can be contact by emailing: dataprotection@hsdc.ac.uk

3.6. **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

3.7. **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.

3.8. **Personal Data** – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held.

3.9. **Processor** – Any entity (e.g., company, organisation, or person) responsible for processing personal data on behalf of a controller.

3.10. **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 and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

4. COLLEGE STAFF'S GENERAL OBLIGATIONS

4.1. All College staff must comply with this policy.

4.2. College staff 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.

4.3. College Staff must not release or disclose any Personal Data:

4.3.1. outside the College; or

4.3.2. inside the College, to College Staff not authorised to access the Personal Data,

without specific authorisation from their manager or the Data Protection Officer; this includes phone calls or emails.

4.4. College Staff must take all steps to ensure there is no unauthorised access to Personal Data, whether by other College Staff who are not authorised to see such Personal Data or by people outside the College.

5. DATA PROTECTION PRINCIPLES

5.1. When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:

5.1.1. processed lawfully, fairly and in a transparent manner;

5.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

5.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

5.1.4. 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;

5.1.5. kept for no longer than is necessary for the purposes for which it is being processed; and

5.1.6. 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.

5.2. These principles are considered in more detail in the remainder of this policy.

5.3. In addition to complying with the above requirements, the College also must demonstrate that it complies with them through documented evidence. The College has several policies and procedures in place, including this policy and the documentation referred to ensure that it can demonstrate its compliance.

6. LAWFUL USE OF PERSONAL DATA

6.1. To collect and/or use Personal Data lawfully, the College needs to show that its use meets one of several legal grounds. Please click here to see the detailed grounds https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing

6.2. When the College collects and/or uses Special Categories of Personal Data, the College must show that one of several additional conditions is met. Please click here to see the additional detailed conditions https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

6.3. The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 6.1 and 6.2. If the College changes how it uses Personal Data, the College needs to update this record and may also need to notify Individuals about the change. If staff, therefore, intend to change how they use Personal Data, they must notify the Data Protection Officer, who will decide whether their intended use requires amendments to be made and any other controls that need to apply.

7. TRANSPARENT PROCESSING – PRIVACY NOTICES

7.1. Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses Personal Data in the form of a privacy notice made available on the College website.

7.2. If the College receives Personal Data about an Individual from other sources, the College can provide the Individual with a privacy notice about how the College will use their Personal Data upon request.

7.3. If the College changes how it uses Personal Data, the College may notify Individuals about the change. If College Staff intends to change how they use Personal Data, please notify the Data Protection Officer who will decide whether the College Staff's intended use requires amendments to be made to the privacy notices and any other controls that need to apply.

8. DATA QUALITY- ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA

8.1. Data Protection Laws require that the College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice (see paragraph 7 above) and as set out in the College's record of how it uses Personal Data. The College is also required to ensure that the Personal Data the College holds is accurate and kept up to date.

8.2. All College Staff that collect and record Personal Data must ensure that the Personal Data is recorded accurately and is kept up to date. College Staff should ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and necessary for the purpose for which it is collected and used.

8.3. All College Staff that obtain Personal Data from sources outside the College must take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date, and limited to that which is adequate, relevant and necessary in relation to the purpose for which it is collected and used.

8.4. To maintain the quality of Personal Data, all College Staff that access Personal Data must ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the College must keep in its original form (e.g., for legal reasons or relevant to an investigation).

8.5. 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 Laws. Any request from an Individual for the amendment, rectification, erasure, or restriction of the use of their Personal Data should be dealt with in accordance with those college processes and procedures relating to Individual rights.

9. PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED

9.1. Data Protection Laws require that the College not keep Personal Data longer than is necessary for the purpose or purposes for which the College collected it.

9.2. The College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the College.

9.3. If College Staff consider that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Schedule, for example because there is a requirement of law, or if College Staff have any questions about the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

10. DATA SECURITY

10.1. The College takes information security very seriously. 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.

11. DATA BREACH

11.1. The College takes information security very seriously; however, it is possible that a security breach could happen, resulting in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens, a Personal Data breach and College Staff must comply with the College's Data Breach Notification Policy. Please see paragraphs 11.2 and 11.3 for examples of what can be a Personal Data breach.

11.2. Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration, or unauthorised disclosure of Personal Data. Most Personal Data breaches happen as a result of action taken by a third party; data breaches can also result from actions taken by College Staff.

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

11.3.1. **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data, e.g. hacking, accessing internal systems that College Staff are 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 incorrect student, or disclosing information over the phone to the incorrect person;

11.3.2. **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 ransomware, 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

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

12. APPOINTING CONTRACTORS/SUPPLIERS WHO ACCESS THE COLLEGE'S PERSONAL DATA

12.1. If the College appoints a contractor or third party that will act as the College's Processor, then Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.

12.2. One requirement of the UK GDPR is that a Controller must only use Processors who meet the requirements of the UK GDPR and protect the rights of Individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed, they should be audited periodically to ensure that they meet their contractual requirements to Data Protection.

12.3. Any contract where an organisation appoints a Processor must be in writing.

12.4. You are considered having appointed a Processor where you engage someone to perform a service for you, and as part of it, they may gain access to your Personal Data. Where you appoint a Processor, you, as Controller, remain responsible for the Personal Data.

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

12.5.1. to only act on the written instructions of the Controller;

12.5.2. to not export Personal Data without the Controller's instruction;

12.5.3. to ensure staff are subject to confidentiality obligations;

12.5.4. to take appropriate security measures;

12.5.5. to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;

12.5.6. to keep the Personal Data secure and assist the Controller to do so;

12.5.7. to assist with the notification of Data Breaches and Data Protection Impact Assessments;

12.5.8. to assist with subject access/Individuals rights;

12.5.9. to delete/return all Personal Data as requested at the end of the contract;

12.5.10. to submit to audits and provide information about the processing; and

12.5.11. to tell the Controller if any instruction is in breach of the UK GDPR or other EU or member state data protection law.

12.6. In addition, the contract should set out:

12.6.1. The subject-matter and duration of the processing;

12.6.2. the nature and purpose of the processing;

12.6.3. the type of Personal Data and categories of Individuals; and

12.6.4. the obligations and rights of the Controller.

13. INDIVIDUALS' RIGHTS

13.1. The UK GDPR gives Individuals more control over how their data is collected and stored and what is done with it.

13.2. The College will use all Personal Data in accordance with the rights given to Individuals under Data Protection Laws and will ensure that it allows individuals to exercise their rights.

13.3. The different types of rights of Individuals are reflected in this paragraph.

13.4. **Subject Access Requests**

13.4.1. Individuals have the right under the UK GDPR to ask the College to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right, but additional information has to be provided, and the timescale for providing it has been reduced from 40 days to one month (with a possible extension if it is a complex request). Also, you will no longer be able to charge a fee for complying with the request.

13.4.2. Subject Access Requests are becoming more and more common and are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

13.5. **Right of Erasure (Right to be Forgotten)**

13.5.1. This is a limited right for Individuals to request the erasure of Personal Data concerning them where:

13.5.1.1. the use of Personal Data is no longer necessary;

13.5.1.2. their consent is withdrawn, and there is no other legal ground for the processing;

13.5.1.3. the Individual objects to the processing, and there are no overriding legitimate grounds for the processing;

13.5.1.4. the Personal Data has been unlawfully processed; and

13.5.1.5. the Personal Data has to be erased for compliance with a legal obligation.

13.5.2. In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the Individual has a right to object to the processing at any time. Where the Individual objects, the Personal Data must not be processed for such purposes.

13.6. **Right of Data Portability**

13.6.1. An individual has the right to request that data concerning them is provided to them in a structured, commonly used, and machine-readable format where:

13.6.1.1. the processing is based on consent or a contract; and

13.6.1.2. the processing is carried out by automated means

13.6.2. This right is not the same as subject access and is intended to give Individuals a subset of their data.

13.7. **The Right of Rectification and Restriction**

13.7.1. Finally, Individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

14. MARKETING AND CONSENT

14.1. The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

14.2. Marketing consists of any advertising or marketing communication that is directed to particular individuals. The UK GDPR will bring about several significant changes for organisations that market to individuals, including:

14.2.1. providing more detail in their privacy notices, including, for example, whether profiling takes place; and

14.2.2. rules on obtaining consent will be stricter and require an individual's "clear affirmative action". The ICO like consent to be used in a marketing context.

14.3. The College conforms with the Privacy and Electronic Communications Regulations (PECR) that sits alongside data protection legislation. PECR applies to direct marketing, i.e., a communication directed to particular Individuals and covers any advertising/marketing material. It applies to electronic communication, i.e., calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data.

14.4. Consent is central to electronic marketing; it is essential to liaise with the Data Protection Officer for best practice recommendations to marketing.

14.5. Alternatively, the College may be able to market using a "soft opt-in" if the following conditions were met:

14.5.1. contact details have been obtained in the course of a sale (or negotiations for sale);

14.5.2. the College is marketing its own similar services; and

14.5.3. the College gives the Individual a simple opportunity to refuse to opt-out of the marketing, both when first collecting the details and in every message after that.

15. AUTOMATED DECISION MAKING AND PROFILING

15.1. Under Data Protection Laws, 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 to evaluate certain things about an Individual.

15.2. Any Automated Decision Making or Profiling that the College carries out can only be done once the College is confident that it complies with Data Protection Laws. Therefore, if College Staff wishes to carry out any Automated Decision Making or Profiling, College Staff must inform the Data Protection Officer.

16. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

16.1. The UK GDPR introduces a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done before the processing via a Data Protection Impact Assessment ("DPIA"). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data. However, it is an assessment of issues affecting Personal Data that need to be considered before a new product/service/process is rolled out. The process is designed to:

16.1.1. describe the collection and use of Personal Data;

16.1.2. assess its necessity and its proportionality in relation to the purposes;

16.1.3. assess the risks to the rights and freedoms of individuals; and

16.1.4. the measures to address the risks.

16.2. 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.

16.3. Where a DPIA reveals risks, which are not appropriately mitigated, the ICO must be consulted.

16.4. Where the College is launching or proposing to adopt a new process, product, or service that involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that the 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 that may otherwise occur.

16.5. Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

16.5.1. large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;

16.5.2. large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences, e.g. the use of high volumes of health data; or

16.5.3. systematic monitoring of public areas on a large scale e.g. CCTV cameras.

16.6. All DPIAs must be reviewed and approved by the Data Protection Officer.

17. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

17.1. Data Protection Laws impose strict controls on Personal Data transferred outside the EEA. A transfer includes sending Personal Data outside the EEA and includes storage of Personal Data or access to it outside the EEA. Giving access to Personal Data to staff outside the EAA needs to be thought about whenever the College appoints a supplier outside the EEA, or the College appoints a supplier with group companies outside the EEA.

17.2. So that the College can ensure it is compliant with Data Protection Laws, College Staff must not export Personal Data unless the Data Protection Officer has approved it.

17.3. College Staff must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

18. ACCOUNTABILITY

18.1. The UK GDPR integrates accountability as a principle, which requires that the College puts in place appropriate technical and organisational measures and be able to demonstrate what it did and its effectiveness when requested.

18.2. The College must demonstrate that it is compliant with the law. Such measures include adequate documentation on what personal data are processed, how, to what purpose, how long; documented processes and procedures are aiming at tackling data protection issues at an early state when building information systems or responding to a data breach; that the Data Protection Officer be involved at the planning stage.