Full name of policy:	**Data Protection Policy**
Requirement for policy:	Legislative Compliance
Name and post of person responsible:	Fi Taylor, Exams Manager
Highest College body approving the policy:	College Leadership Team
Date of approval:	
Frequency of review:	Every 2 years (or as legislation changes)
Dates of previous reviews:	November 2011, October 2013,
Date of next formal review:	March 2018
Equality Impact Screening:	Yes
Equality Impact Assessment: (If required)	Not required
Policy Reference:	All policies can be located on the U drive/SDC Policies folder
Total number of pages: (Including appendices and front sheet)	13 pages
Comments:	This policy should be read in conjunction with: • Data Protection Guidance for Staff; • Data Protection FAQ and Best Practice Guidance; • Other Data Protection Guidance available on the U drive /Information Services • Network Services Regulations (Various documents); • Freedom of Information Policy; • Safeguarding Policies (Adults at Risk and Young Persons). • SDC Information Security Policy

SUSSEX DOWNS COLLEGE - DATA PROTECTION POLICY

1. Introduction

1.1. Summary

Sussex Downs College is required to keep certain information about its employees, students, partners and other users to allow it to monitor recruitment, performance and achievements. It is also necessary to process information so that the College can comply with its legal obligations, staff can be recruited and paid, and courses organised and delivered.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. This is relevant whether the information is collected, recorded and used on paper, electronically or by other material.

To do this, Sussex Downs College must comply with the Eight Data Protection Principles as set out in the Data Protection Act 1998 (the Act).

1.2. The Eight Principles of Data Protection

The Principles require that personal data shall:

Principle 1:
Be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions as laid out in the Act are met. In the case of sensitive personal data there are further conditions that must also be met. (Please see Appendix A and B for details of the conditions and Appendix C for details of exemptions)

Principle 2:
Be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes for which they are processed.

Principle 3:
Be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle 4:
Be accurate and, where necessary, kept up to date

Principle 5:
Not be kept for longer than is necessary for that purpose or those purposes for which they are processed

Principle 6:
Be processed in accordance with the rights of data subjects under the Act

Principle 7:
Be kept safe from unauthorised access, accidental loss or destruction.

Principle 8:
Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. (Please see Appendix D)

1.3. Purpose

The purpose of this policy is to enable SDC to:

- comply with the law in respect of the data it holds about individuals;
- follow good practice;
- protect the rights of students, staff and other individuals;

- protect the organisation from the consequences of a breach of its responsibilities;
- be open and honest with the individuals whose data is held;
- provide training and support for staff who handle personal data, so that they can act confidently and consistently

SDC recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. In the main this means:

- keeping information securely and in the right hands
- holding good quality information

1.4. *Status* of this Policy

This policy does not form part of the formal contract of employment for staff, or the formal offer of a place of study for students, but it is a condition of employment or study that employees and students will abide by the rules and policies made by the College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

1.5. Key risks

SDC has identified the following potential key risks, which this policy, associated guidance and other related policies are designed to address:

- Breach of confidentiality (information being given out inappropriately)
- Insufficient clarity about the range of uses to which data will be put, leading to Data Subjects being insufficiently informed
- Failure to offer choice about data use when appropriate
- Breach of security by allowing unauthorised access within the organisation
- Failure to establish efficient systems of managing changes to information held leading to personal data being not up to date
- Harm to individuals if personal data is not up to date
- Accidental loss or destruction of data and associated breach of security
- Breach of security through the inappropriate storage or transport of data

2. Responsibilities

2.1. Board of Governors

The College as a body corporate is considered to be the Data Controller under the Act, and the Governors are therefore ultimately responsible for implementation and oversight of this policy. Their responsibilities are for ensuring that data is collected, stored and processed fairly, for deciding which types of information will be processed and the reasons for processing.

2.2. The Principal and College Leadership Team

It is the responsibility of the Principal and College Leadership Team to approve this policy and ensure compliance with the policy and for communicating the policy to all staff.

2.3. The Data Controller

The Designated Data Controller for the College is the Exams Manager, who has operational responsibility for the implementation of this policy, and is responsible for day-to-day data protection matters, providing advice, developing data protection guidance and raising awareness of data protection matters across the college.

2.4. Leaders/Managers/Supervisors

All managers are responsible for ensuring that staff in their area are aware of and abide by this policy and associated guidance and ensuring their teams attend training as appropriate. Additionally they are responsible for the security of information within their area and for adopting and encouraging good information handling practice within the College.

2.5. All Staff

All staff are responsible for ensuring that any personal data which they hold is kept securely and personal information is not disclosed accidentally or otherwise to any unauthorised third party.

If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course work, opinions about ability, work or academic references, or details of personal circumstances), they must comply with the data protection principles, defined under the Act and as set out in this policy.

All staff have a responsibility to make themselves aware of and abide by this policy and associated guidance and attend or participate in training as required.

2.6. All Students and Staff (as data subjects)

Learners and staff are responsible for ensuring that all personal data provided to the College is accurate and up to date. It is their responsibility for informing the college when this changes.

3. Definitions under the Act

3.1. Personal Data

Data relating to a living individual where on its own or together with other readily accessible data enables the identification of an individual. This includes name, address, telephone number, id number. It also includes expression of opinion about the individual.

3.2. Sensitive Data

Different from ordinary personal data and relates to racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical or mental health, sexual orientation, age, gender identity, criminal convictions or allegations of such. Sensitive data are subject to much stricter conditions of processing.

3.3. Data Subject

Any living individual who is the subject of personal and or sensitive data held by the college.

3.4. Third Party

Any Individual or organisation other than the data subject, the data controller (The College) or its agents.

3.5. Processing

Any operation related to organisation, retrieval, disclosure and deletion of data and includes:

- Obtaining and recording data
- Accessing, altering, adding to, merging, deleting data
- Retrieval, consultation or use of data
- Disclosure of or otherwise making available data

3.6. Relevant Filing System

Any paper or other manual filing system which is structured so that information about an individual is readily accessible. In certain circumstances it may also apply to unstructured personal data that is held.

This is the definition of "Relevant Filing System" in the Act. However personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

4. Rights to Access Information

4.1. Rights of Data Subjects

All staff, students and other users are entitled to:

- Know what information the College holds and processes about them and why
- Know how to gain access to it

- Know how to keep it up to date
- Know what the College is doing to comply with its obligations under the Act

4.2. Requests for Access to Information

The College will, upon request, provide all staff and students and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the College holds and processes about them, and the reasons for which they are processed. (A standard list is attached as Appendix E).

Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should do so in writing to the college. This may be in the form of a letter, email or by completion of a Subject Access Request Form, which should be submitted to the appropriate person (Example form attached as Appendix F). If there is any doubt about the identity of the person making the request the college will request further evidence to reasonably confirm their identity.

4.3. College Response to Requests

The College will make a charge of £10 on each occasion that access is requested, although the College has discretion to waive this.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that a response is provided within 40 working days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

4.4. Examination Marks

During the course of their studies, students will routinely be provided with information about their marks for both coursework and examinations. However, exam scripts themselves are exempted from the subject access rules and copies will not ordinarily be given to a student who makes a subject access request.

5. Subject Consent

5.1. Definition of Consent

The College understands "consent" to mean that the data subject has been fully informed of the intended processing and has freely signified their agreement. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form. Consent cannot be inferred from non-response to a communication.

5.2. Processing Personal Data

One of the conditions for processing data is that it is carried out with the consent of the data subject.

It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the world. Therefore, not gaining consent could contravene the eighth data protection principle. This also applies to the publication of photographs.

Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

5.3. Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, or to meet our legal obligations. Photographs are considered sensitive information as they may reveal a person's race, gender or other physical characteristics.

Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, Staff and students will be asked to give express consent for the College to do this.

Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason.

5.4. Collection of consent

In most instances consent to process personal and sensitive data is obtained routinely by the College (e.g. when a student signs a Learning Agreement). Any College form (whether paper-based or web-based) that gathers data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed.

5.5. Withholding Consent

If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

5.6. Safeguarding

Many jobs or courses will bring the applicants into contact with young people between the ages of 14 and 18. The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered.

The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use the College facilities do not pose a threat or danger to other users. Please refer to the College Safeguarding Policy for more details.

5.7. Further information

If a student or any member of the College is in any doubt about these matters, they should consult an appropriate member of staff (e.g. Tutor, Line Manager or Designated Data Controller).

6. Data Security

All personal data should be accessible only to those who need to use it. Staff should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- in a lockable room with controlled access - or
- in a locked drawer or filing cabinet - or
- if computerised it should be password protected, encrypted or access controlled and be regularly backed up - or
- if kept on portable storage media they are themselves kept securely and password protected

Care should be taken to ensure that PCs and terminals screens are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

This policy also applies to processing personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Particular care should be taken when processing personal data at home or in other locations outside the College campus and in the transportation of personal data between sites.

Each area (as defined on the College Organisation and Management Structure) is responsible for the security of the data they hold, and for the safe storage, retrieval, archiving and appropriate destruction of that data, in line with the guidance for the Retention of Personal Data as set out in Appendix G of this policy.

7. Publication of College Information

Information that is already in the public domain is exempt from the Act. When any statute or law require such data to be made public the names of Senior Managers and Governors of the College and other relevant information about the college and its business are published on the public Web site. More information is available in the Freedom of Information Policy and on the College web site.

8. Retention of Data

The College has a duty to retain some staff and student personal data for a period of time following their departure from the College, mainly for legal reasons, but also for other purposes such as being able to provide references, or for financial reasons, for example relating to pensions and taxation potential or current disputes or litigation.

Different categories of data will be retained for different periods of time. The exact details of retention periods and purposes are set out in Appendix G.

9. Disposal of Records

All areas should conduct regular audits on the data they are holding, and arrange for secure and appropriate disposal. Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion of hard drives or portable storage devices).

10. Conclusion

Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated data controller.

11. Addendum

The College is in the process of writing information security, records retention and archiving, and data sharing policies. In the meantime any issues relating to these should be taken up with the designated data controller

Appendix A – Conditions of Processing Personal Data

The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

- The individual who the personal data is about has consented to the processing.
- The processing is necessary:
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract)
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
- The processing is in accordance with the "legitimate interests" condition

Appendix B – Conditions of Processing Sensitive Personal Data

If the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle. These other conditions are as follows:

- The individual who the sensitive personal data is about has given explicit consent to the processing
- The processing is necessary so that you can comply with employment law
- The processing is necessary to protect the vital interests of:
  - the individual (in a case where the individual's consent cannot be given or reasonably obtained)
  - another person (in a case where the individual's consent has been unreasonably withheld)
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition
- The individual has deliberately made the information public
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights
- The processing is necessary for administering justice, or for exercising statutory or governmental functions
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality
- The processing is necessary for equality and diversity monitoring and reporting purposes which ensure that the College fulfils its statutory duties as set out in the Equality Act 2010

In addition to the above conditions – which are all set out in the Data Protection Act itself – regulations set out several other conditions for processing sensitive personal data. Their effect is to permit the processing of sensitive personal data for a range of other purposes – typically those that are in the substantial public interest, and which must necessarily be carried out without the explicit consent of the individual. Examples of such purposes include preventing or detecting crime and protecting the public against malpractice or maladministration. A full list of the additional conditions for processing is set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000 and subsequent orders.

Appendix C - Exemptions

It is assumed that all personal information collected and processed by the college is subject to the data protection Act (1998). However in some circumstances, such as there is some public interest involved, data may not be affected by the act. Examples include:

- National security
- Journalism, where publication is in the public interest
- Crime and Taxation
- Regulatory activity
- Confidential references
- Management forecasting or planning
- Examination marks and personal data contained in examination scripts
- Personal data that consists of educational records

There are other exemptions described and explained in detail on the ICO website

Entitlement to an exemption depends in part on the purpose for processing the personal data in question, for example, there is an exemption from some of the Act's requirements about disclosure and non-disclosure that applies to processing personal data for purposes relating to criminal justice and taxation. However, each exemption should be considered on a case-by-case basis because the exemptions only permit a departure from the Act's general requirements to the minimum extent necessary to protect the particular functions or activities the exemptions concern.

Appendix D - European Economic Area (EEA)

The Eight Principle of the Data Protection Act states that personal data shall not be transferred to a country or territory outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The EEA consists of the member states of the European Union together with Iceland, Liechtenstein and Norway. A list of the current member states may be found at:
http://www.dwp.gov.uk/international/social-security-agreements/list-of-countries/

Unless absolutely necessary data should not be transferred outside of the EEA, should it be deemed necessary the person responsible shall ensure that appropriate security measures are taken.

Appendix E - List of the standard set of information held by the college

Staff: (in some cases not all those listed will apply)

Name, address, phone number and email address
Date of birth, age, gender and ethnicity
Job application details
Bank details
Pension arrangements
Wages and Salary records
NI and Income tax records
Staff appraisal details
Training and qualification records
Attendance and sickness records
Disciplinary and grievance records (where applicable)
Health and/or medical records (where applicable)
Accident reports (where applicable)
Records of maternity, paternity or parental leave (where applicable)
Records of DBS checks (where applicable)
Photograph

The above records are held in order to appropriately manage the employment, pay and conduct of members of staff and to comply with legal requirements relating to employment and health and safety.

Students (in some cases not all those listed will apply)

Name, address, phone number and email address
Date of birth, age, gender and ethnicity
Country of residence and status of UK/EU residence
National Insurance number (where applicable)
Details of prior attainment and average GCSE score
Details of benefits in relation to waiver of tuition fees (where applicable)
Learning difficulties and/or disabilities information
College application details (including academic reference from previous school)
Course Enrolment details
Academic progress, assessment and achievement details
Attendance details
Conduct and disciplinary records (where applicable)
Details of additional learning support needs and provision (where applicable)
Health and/or medical records (where applicable)
Accident reports (where applicable)
Prior and/or current employment details
Details of means tested assessment (for the administration of the discretionary learning support fund (DLSF) and the 24+ Advanced Learning Loans Bursary; 16-19 Bursary Fund – which consist of Vulnerable Student Bursaries and Discretionary Bursaries)
Destination information
Photograph

The above records are held in order comply with the statutory duty of the college to make data returns to the Funding Agencies. In addition records are held to monitor the progress and performance of students; provide support and assistance to students in the course of their study; to monitor the recruitment, performance and achievement of the student body. Records are also held to comply with legal obligations with regard to equal opportunities, equality and diversity, safeguarding, and health and safety.

Appendix F – Subject Access Request Sample Form

Personal Information Request Form

The Data Protection Act 1998 gives an individual the right to request the college for a copy of the personal information that we hold about you. You are not entitled to see information that we hold about a third party without their consent. Please note that the College reserves the right to obscure or suppress information that relates to other third parties (under Section 7 of the Data Protection Act 1998) when providing information based on this request.

Under the Data Protection Act 1998 the college has the right to charge a fee of £10 for providing data requested on this form. Where applicable payment will be required prior to the release of information, and should be enclosed when submitting this form (cash, cheque- payable to SDC or postal orders are acceptable). For current staff or students this fee would usually be waived however the college reserves the right to make this charge in certain circumstances. The college will endeavour to respond to requests within 40 working days from the receipt of this Personal Information Request Form, appropriate supporting documents and payment where applicable. However where further information is required in order to process this request it may take longer.

Details of the person requesting information:

Name				
Address **Post Code**				
Contact Telephone Number(s)		**Email address**		
Student Number (if Applicable)			**Member of Staff?**	
Course			**Campus**	
Dates of Study/Employment:	**From**		**To**	

Are you the Data Subject?

YES	If you are the Data Subject please supply evidence of your identity, e.g. Photocopy of your driving licence, Passport, original bank statement or utility bill and if necessary a stamped addressed envelope for returning the document once your request has been processed. If you are a current member of staff or student please provide a copy of your ID card.
No	Are you acting on behalf of the Data Subject? If so please provide their written authority and evidence of their ID as detailed in the box above, with this form

Details of the data subject (if different to above):

Name				
Address **Post Code**				
Contact Telephone Number(s)		**Email address**		
Student Number (if Applicable)			**Member of Staff?**	
Course			**Campus**	
Dates of Study/Employment:	**From**		**To**	

If you are not the data subject, please describe your relationship to the data subject that leads you to make this request for information on their behalf:

Please give details of the information you require, together with any additional information which may help us to locate it. If you wish to see only certain specific document(s), please describe these below:

Declaration

I certify that the information given on this application form to is true and accurate. I understand that it is necessary for the College to confirm my/ the Data Subject's identity and it may be necessary to obtain more detailed information in order to locate the correct information requested.

Name:_____ **Signed**_____ **Date** _____

Office Use Only:

Ref:		**Date Request received**	
Date Due		**Date Completed**	
Notes			

Appendix G – Guidelines for the Retention of Personal Data

Type of Data	Suggested Retention Period	Reason
Personnel files including training records and notes of disciplinary and grievance hearings.	6 years from the end of employment	References and potential litigation
Application forms/interview notes	6 months – one year from the date of the interviews.	Time limits on litigation
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy	As above
Income Tax and NI returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity, Parental Pay, Adoption Pay, Sick Pay and similar records and calculations	6 years	Time limits on contract litigation
Wages and Salary records	6 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	Up to 40 years	RIDDOR 1985
Health records	During employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress related illness.	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances Hazardous to Health Regulations 2002	Up to 40 years	COSHH REGULATIONS 2002
EFA Funded: - Student records, including academic achievements, and conduct.	At least 6 years from the date the student leaves the College, in case of litigation for negligence, At least 10 years for personal and academic references.	Limitation period for negligence.
ESF Funded and co-financed provision requires: - Student records documentation - Publicity materials - Equal Opportunities and Sustainability Policies	A much longer retention period is needed as detailed in contracts, this is currently until 31st December 2030 for the 2014-2020 ESF Programme, but relates to documents from the 2015-2016 academic year onwards	Contractual obligation

Appendix H - Further information and Useful Websites

- College Website
  http://www.sussexdowns.ac.uk/policies.htm
  http://www.sussexdowns.ac.uk/aboutus/foi.htm

- On the college U Drive:
  U:\Information Services\Data Protection Act and FoI Act\
  SD College Policies and Guidelines
  SDC Internet acceptable use policy
  SDC Email acceptable use policy
  SDC IT acceptable use policy

- Data Protection Tools and Resources
  https://search.ico.org.uk/ico/search

- The Complete Data Protection Act can be viewed at:
  http://www.legislation.gov.uk/DPA_1998

- Information Commission:
  https://ico.org.uk/global/contact-us/

- European Economic Area (EEA)
  http://www.dwp.gov.uk/international/social-security-agreements/list-of-countries/

- Freedom of Information Act:
  https://ico.org.uk/about-the-ico/what-we-do/freedom-of-information-act/