South Downs College

DATA PROTECTION POLICY

Responsible Senior Manager:	Assistant Principal Finance & Facilities *
Approved by:	Governors
Date Approved:	3 March 2016
Related Policies:	Information Security Policy Acceptable Use of ICT Policy Retention & Disposal Procedure Freedom of Information Scheme Admissions Policy Public Interest Disclosure (Whistleblowing) Procedure Safeguarding Policy Disciplinary Procedure
Next Review Date:	January 2019

* The Vice Principal will be the designated Data Controller pending permanent appointment of Assistant Principal Finance & Facilities

SOUTH DOWNS COLLEGE

DATA PROTECTION POLICY

1. Policy Statement

South Downs College is required to retain certain information about its employees, learners and other users in order to facilitate the monitoring of performance, achievements, and health, safety and wellbeing. The College is also expected to comply to the anti-terrorism Prevent agenda 2015. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information stored in files (either paper based or electronically including on a computer including e-mail, internet, intranet or portable storage device) covered by the data protection legislation must be collected and used fairly, stored and disposed of safely, and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act).

In summary these state that personal data shall:

1.1 Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.

1.2 Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

1.3 Be adequate, relevant and not excessive for those purposes.

1.4 Be accurate and kept up to date.

1.5 Not be kept for longer than is necessary for that purpose.

1.6 Be processed in accordance with the data subject's rights.

1.7 Be kept safe from unauthorised access, accidental loss or destruction.

1.8 Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed the Data Protection Policy, adherence to which is compulsory for all staff.

2. Scope

This policy applies to all members of the College community (staff (including agency workers), governors, learners, contractors/suppliers, volunteers, shared services providers and members of the public).

This policy does not form part of the formal staff contract of employment nor of the student contract with the College, but it is a condition of both contracts that College regulations and policies must be adhered to. A failure to follow the policy may result in disciplinary proceedings.

Any members of staff or learners who consider that the policy has not been followed in respect of personal data about themselves or about other data subjects should raise the matter with the designated Data Controller (see paragraph 5.3) initially (learners may wish to do this through their lecturer or course tutor). If the matter is not resolved it should be raised as a formal complaint or grievance or through the College's Public Interest Disclosure (Whistleblowing) Procedure where appropriate.

3. Definition of Terms

Data Subject – A Data Subject is a living person who has information recorded about them.

Data Controller – A Data Controller is an organisation, or individual, who is responsible for determining why personal data is processed and also for the manner in which it is processed. The data controller can be a company, government department, organisations or they can be individuals such as GP's and pharmacists.

Data Processor – A Data Processor is any person (other than employee of the Data Controller) who processes the data on behalf of the Data Controller. An example of a Data Processor would be an external payroll company used by an organisation to process payments for their employees. The payroll company would have to handle personal information to carry out payment tasks but would not exercise control over the personal data supplied.

Data Recipient – A Recipient is any person who views data in the course of its proceedings by, or on behalf of, the Data Controller. This can include an employee or agent of the Data Controller or an employee or agent of the Data Processor. However, this definition excludes any person who views data as a result of a legal investigation.

Third Party – A Third Party is defined as any person other than the Data Subject, the Data Controller, The Data Processor or any other person authorised to process data for the Data Controller of Data Processor.

4. Legislation

- Data Protection Act 1998
- The Freedom of Information Act 2000
    - The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
    - The Freedom of Information (Time for Compliance with Request) Regulations 2004
    - The Freedom of Information (Removal and Relaxation of Statutory Provisions on Disclosure of Information) Regulations 2004
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 and subsequent Amendments 2004, 2011 and 2015

- Computer Misuse Act 1990
- Education Act 2002
- Counter-Terrorism and Security Act 2015, Prevent Agenda
- The Environmental Information Regulations 2004
- The INSPIRE Regulations 2009
- Re-use of Public Sector Information Regulations 2015
- The Protection of Freedoms Act 2012

5. Responsibilities

5.1 All College staff have responsibility for

i. Checking that information they provide to the College in connection with their employment is accurate and up to date.
ii. Informing the College of changes to information which they have provided, e.g. change of address.
iii. Checking the information that the College will send to them from time to time, which gives details of information kept and processed about them.
iv. Informing the College of any errors or changes. The College cannot be held responsible for any errors which staff members have had the opportunity to correct.

5.2 If and when, as part of their responsibilities, staff collect information about other people (i.e. learners' course work, opinions about ability, references to other academic institutions, or details of personal circumstances) they need to follow the Data Protection Principles and they must comply with the College guidelines for staff, which are at Appendix A.

5.3 The Data Controller and the designated Data Controller - The College as a Body Corporate is the Data Controller under the Act and the Board of Governors is therefore ultimately responsible for ensuring implementation of the Act. The designated Data Controller is the Assistant Principal Finance & Facilities, who will deal with day to day matters.

The Assistant Principal Finance & Facilities has overall responsibility.

6. Actions to Implement and Develop Policy

6.1 Notification of Data Held and Processed

All staff, learners and other data subjects 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 1998 Act

The College will advise staff and learners and other relevant data subjects about the types of data the College holds and processes about them, and the reasons for which it is processed. This will be notified via application/enrolment or other documentation.

The College utilises Closed Circuit Television Systems across site for Security and Safeguarding purposes, in line with relevant legislation and following current best practice for the operation of such systems.

6.2 Information Security

All staff have responsibility for ensuring that:

- Any personal data which they hold is stored and disposed of securely.

- Personal information is not disclosed orally, in writing, accidentally, or otherwise to any unauthorised third party.

  Staff should note that unauthorised disclosure is a disciplinary matter and may be considered gross misconduct in some cases.

  Personal information should be stored securely, usually this means

  - In a locked office, or
  - In a locked filing cabinet, or
  - In a locked drawer, or
  - If it is computerised, be password protected, or
  - If it is kept on portable storage (i.e. USB, laptop, etc) be both encrypted and password protected and itself kept securely

  The Head of Information Technology should be consulted for guidance on storage, transmission, encryption and disposal of data owned by the College.

  The College reserves the right to monitor and report on all electronic / written communication that could be linked to terrorism (Prevent agenda).

6.3 Unauthorised Access

Any member of staff or student who deliberately gains or attempts to gain unauthorised access to personal data on any data subject or discloses such data to any third party may be disciplined in accordance with College procedures.

6.4 Student Obligations

Learners must ensure that all personal data provided to the College are accurate and up to date. Learners must ensure that changes of address, etc, are notified via Curriculum administration staff or the Data Management team.

Next of Kin Information – If a student has chosen to withhold next of kin information – the College will inform the Police in the event of an emergency or accident.

Prevent – If the College is concerned that a student could be linked to terrorism or incitement of terrorism – The College is legally required to advise the Police.

6.5 Rights of Access to Information

Staff, learners and other data subjects have the right of access to any personal data that are being kept about them either on computer or in certain other files. Any person who wishes to exercise this right should complete the College "Data Access Request" form (see Appendix B) and send it to the designated Data Controller or, in the case of a student, to her/his course tutor or lecturer. Forms are available from the Finance Office.

The College will make a charge of £10 on each occasion that access is granted, although it has discretion to waive this charge for good reason at the discretion of a member of the College Senior Leadership Team.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within the statutory time limit of 40 calendar 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.

To request access to general information (non-personal information) held by the College, a Freedom of Information request should be made.

6.6 Requests for Access by 3rd Parties

The Data Protection Act includes a number of non-disclosure exemptions, these include:

- Prevention and detection of crime, capture or persecution of offenders, assessment or collection of tax or duties.
- Regulatory activity, for example, protecting members of the public from dishonesty, malpractice, incompetence of improper conduct.
- Disclosure required by law, such as an order of court.
- In connection with legal proceedings, obtaining legal advice and defending legal rights.
- Prevent (anti-terrorism).

Where a 3rd party, such as the Police / makes a request for data under one of the above exemptions, the Assistant Principal Finance & Facilities (or College Principal) will approve in writing access to this material.

No data shall be released without written consent.

6.7 Public Domain

Information that is already in the public domain is exempt from the 1998 Act.

6.8 Subject Consent

In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data are sensitive, express consent must be obtained.

Data is considered sensitive if it is about an individual's race; political opinions; religious beliefs; trade union membership; health; sex life or criminal record.

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 convictions.

Some jobs or courses will bring the applicants into contact with children, including young people aged 17 or below or vulnerable adults. The College has a duty under the Education Act 2002 and other enactments to ensure that staff are suitable for the job, and learners for the courses offered. The College also has a duty of care to all staff and learners and must therefore make sure those employees, and those who use the College facilities, do not pose a threat or danger to other users.

The College will also ask for information about particular health needs, such as allergies to particular forms of medication or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff and learners will be asked to sign a 'Consent to Process' clause in any application forms, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

6.9 Examination Marks

Learners will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide.

6.10 Retention of Data

A full list of information with retention times is available from the designated Data Controller and detailed in the Retention and Disposal Procedure.

The College will only need to keep information as long as it is lawfully required to do so; for example, see requirement of the ESF programme below.

Some information, including information about health, or disciplinary matters will be destroyed within 3 years of the learners leaving the College.

The College will need to keep information about staff for six years after the employment ceases. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, health, potential or current disputes or litigation regarding the employment and information required for job references.

European Social Fund (ESF) – Retention of Documents

The College and its sub-contractors shall retain original invoices, management information returns and all other documents necessary to verify the Provision delivered by itself or by its sub-contractors in relation to the Skills Funding Agency Financial Memorandum 2015-16 for 6 years from the end of the financial year in which the last payment is made.

Where the provision has been funded using monies from the European Social & Investment Funds (ESIF), or where any payments made under the Financial Memorandum for the Provision have been used as match-funding for a ESIF Project, the College will be required to retain all documents necessary to verify the delivery of the Provision by itself or by its sub-contractors. Documents to support claims must be retained for a minimum of three years after the European Commission has made its final payment. For the 2007-13 ESF programme this is expected to be until 31 December 2022 and for the 2014-20 ESF programme until at least 31 December 2030.

Confirmation of the destroy date will be notified in writing by the SFA. Without prejudice to any of the other rights under the Financial Memorandum to recover funds, the SFA will be entitled to recover from the College any sums which it is required to repay to the European Social Fund as a result of the College's failure to comply with this Clause.

6.11 Payment Card Industry (PCI) Compliance

A very important aspect of our Data protection responsibilities relates to PCI Compliance.

There are strict industry requirements governing processing payments by Credit or Debit card which anyone involved with such transactions must adhere to. These are necessary to maintain security within the payment card industry. Organisations incur financial penalties if they cannot demonstrate robust processes to protect payment and information.

Within the College, any person involved with taking payments by card must ensure that they understand the requirements. Such transactions might include payments for:

- Theatre box office
- Catering restaurant/shop
- Hair and beauty salon
- Reception
- Supplier payments
- Enrolments via Friendship Centre
- Reprographics

This does not include payment made by using WisePay, eg for educational visits, as this system has been independently verified as PCI compliant.

Further information on PCI Compliance can be found at: www.pcisecuritystandards.org

7. Actions to be Taken in the Event of a Security Breach

In the case of a data breach, the Data Controller will need to judge the severity of the breach. The areas of consideration in this judgement are:

- The potential damage to the individuals.
- The volume of personal data affected.
- The sensitivity of the personal data.
- Was there a justifiable need to remove the data?

The severity options are:

- Not Severe – Justified
- Not Severe – Unjustified
- Severe – Justified
- Severe – Unjustified

Action to be taken:

Not Severe – Justified
With all data movement there is a risk. If a breach occurs at this time and it is felt that the data is not sensitive or severe in its loss then the data controller can choose to take no further action

Not Severe – Unjustified
Any unjustified removal of data, will result disciplinary action in line with the colleges Information Security policy.

Severe – Justified
In the case of a severe breach the Information Commissioners Office (ICO) will need to be notified. The ICO will advise the data controller on the next steps to take. As with the not severe – Justified above the data controller can choose to take no further disciplinary based action

Severe - Unjustified
In this circumstance, as with the Severe – Justified, the ICO must be notified. The ICO will consider the case and advise the data controller on the next steps. The data controller will also follow the disciplinary actions as laid out in the Information Security Policy. The ICO can choose in these circumstances to prosecute the individual responsible for the breach.

Equality Impact Assessment:

SOUTH DOWNS COLLEGE EQUALITY IMPACT ANALYSIS	**DATE: Sept 2015**
Function: Data Protection	
This policy, plan, procedure, process has been examined for equality impact, i.e, the impact that this function will have on different groups of actual and potential learners, service users and staff taking account of the protected characteristics of the Equality Act 2010 **(age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation).**	
1. **If Equality Impact Analysis is not relevant to this function, give reasons and proceed to section 5 below.**	
2. **In what ways could this function have a negative impact on any of the groups above? What actions have been taken to eliminate these?** No adverse impact as the policy outlines the legislative requirement in relation to personal data in accordance with the Data Protection Act 1998 and affects all staff/students, etc, equally.	
3. **In what ways could this function have a positive impact on any of the groups above? How will this function be used to eliminate discrimination, advance equality of opportunity and foster good relations between different groups? Are there plans for the future which will further advance equality?** To protect the rights and privacy of individuals including staff, students and other data subjects in accordance with the DPA 1998. This policy provides a framework for responsible behaviour by those using personal and sensitive information.	
4. **What evidence supports your judgment e.g. consultations, observations, expert opinions, quantitative or qualitative surveys? If the evidence is in the form of an additional document, where is it stored?** In consultation with the College Senior Leadership Team and Governors and reviewed periodically with them. It will be shared with staff through training.	
5. **Name and job title of manager responsible:** Assistant Principal Finance & Facilities	

South Downs College

STAFF GUIDELINES FOR DATA PROTECTION

1. All staff will process data about students on a regular basis, when marking registers, or College work, writing reports or references, or as part of a pastoral or academic supervisory role. The College will ensure through registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 1998 Act. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

    - General personal details such as names and address.
    - Details about class attendance, coursework marks and grades and associated comments.
    - Notes of personal supervision, including matters about behaviour and discipline.

2. Information about a student's physical or mental health; sexual life; political or religious views, trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent, e.g. recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties.

3. All staff have a duty to make sure that they comply with the data protection principles, (see Introduction to Policy). In particular, staff must ensure that records are:

    - Accurate.
    - Up-to-date.
    - Fair.
    - Kept and disposed of safely, and in accordance with the College policy.

4. Staff will be responsible for ensuring that all data is kept securely.

5. Staff must not disclose personal data to any student (or legally-appointed advocate), unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with the College policy.

6. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with College policy.

7. Before processing any personal data, all staff should consider the checklist below.

Staff Checklist for Recording Data

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent (or the consent of his/her or appropriate representative/carer)?
- Has the student been told that this type of data will be processed?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?

Public Facing Operations

Staff involved in “public-facing” operations (eg Theatre Box Office, Restaurant, Hair & Beauty Salons, Fitness Centre) must ensure that they comply with the Data Protection Act and College Policy. In particular, if these operations involve the processing of card payment transactions, steps must be taken to ensure PCI compliance.

Guidelines for Use of Laptops and Memory Sticks

1. Personal data MUST NOT be removed from the premises unless this is essential; if it is essential then any risk should be assessed and sensitive data MUST be encrypted and password protected.
2. Laptops and memory sticks which regularly hold sensitive personal data MUST be fully encrypted.
3. If only a few files are sensitive it may be feasible simply to encrypt those files rather than the whole disk. This could be done on the laptop or memory stick.

Data Access Request Form

Name	
Organisation	
Telephone	
Mobile Phone	
E-Mail	
Contact Address	

Description of Information Being Requested

Data Protection Act Exemption Reason	
Prevention & Detection of Crime	
Regulatory Activity	
Disclosure Required by Law	
Legal Advice/Proceedings	
Contractual Agreement	
Other (please specify)	

Signature	
Date	

Please return this form to the address below together with payment of £10 (cheques should be made payable to South Downs College) and evidence of your identity as to Data Subject, or documentation that confirms your entitlement to act on the Data Subject's behalf (eg a signed form of authority or power of attorney).

OFFICE USE ONLY

Received By		Date		Signature	
Approved By		Date		Signature	
Encryption Required? (Y/N)					