POLICY

Policy name:	Data Protection
Date:	March 2018
Author:	Margaret Ridge
Consultation group:	Representatives from curriculum and support managers who have constituted the GDPR steering group.
This policy is relevant to (tick as applicable):	Students ☒ Governors ☒ Staff ☒ Employers ☒
Policy to be located:	College Intranet

Is SLT approval required?	YES ☒ NO ☐
Approved by:	SLT
Date of approval:	
Reference number: (to be allocated by Governance and Admin):	
Date to be reviewed: (to be agreed at approval):	

1. POLICY STATEMENT

The College needs to keep certain information about its employees, students, and others in order to allow it to conduct its legitimate business.

It is necessary to process information so that staff can be recruited and paid, performance, achievements and health and safety monitored, courses organised in order to fulfil contracts with students, and to comply with legal obligations to funding bodies and other government agencies.

The college processes personal data both as a Data Controller and as a Data Processor. For all government funded activity undertaken, the college is a Data Processor for the ESFA who is the Data Controller. The college is the Data Controller for all other activity such as employment

records and non government funded student activity.

To comply with the Data Protection Legislation, and specifically with General Data Protection Regulations (GDPR), personal information is collected and used fairly, stored safely, and not disclosed to any other person or organisation unlawfully. To do this, the College complies with the requirements of the Data Protection Act 1998 and GDPR 2018.

The college is transparent about the purposes for which personal data is processed and has clearly articulated Privacy Statements, Information Asset Register and Data sharing agreements and index.

The college embraces the concept of Privacy by Design and has systems in place to ensure that any new system / activity undergoes Privacy Impact Assessment (PIA)

The college is currently registered with the Information Commissioner's Office and will continue to be registered, post GDPR implementation, until December 2018 when the college's current registration expires. Following expiry, the college will comply with the new legal requirement to pay the relevant ICO fee only.

Currently the Data Protection registration number for City of Sunderland College is Z7456751. The College's entry on the register can be viewed at http://www.ico.gov.uk/for_organisations.aspx

The Lawful Bases upon which the college relies for its processing of personal data are primarily:-

Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Public task: The processing is necessary for the college to carry out it's official functions.

In some circumstances, consent may be requested from data subjects.

2. STATEMENT OF PRINCIPLES

The college adopts the principles outlined within GDPR and has systems and processes to ensure compliance with these.

At Sunderland College it is ensured that personal data is:-

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

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.

3. EXPLANATION OF KEY TERMS

Consent- requires that there is an active agreement between the organisation and the data subject. Where consent is obtained, it must be explicit and not implied if the subject does not actively object.

Data controller - A data controller determines the purposes and means of processing personal data.

Data processor - A processor is responsible for processing personal data on behalf of a controller

Data subject - An identifiable natural person who can be identified, directly or indirectly form data held.

Personal data - Personal data means information about a natural person who can be identified from that information and other information which is in, or likely to come into, the data controller's possession

Processing - Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data.

Relevant Filing System - This is a set of information about individuals, held manually or on a computer, which is structured either by name or by another criterion, such as a course title so that specific information is readily accessible to the person using or processing.

Sensitive Data (Special Category) - Data is considered sensitive if it about an individual's race, political opinions, religious beliefs, trade union membership or non membership, their physical or mental health, sex life or criminal record.

Data subjects rights - Under GDPR, data subject's rights are enhanced. Individuals can ask to see the information about themselves that is held on computer and in some paper records. They have the right to receive this information in an electronic, accessible format, free of charge, within 1 month of the request being made. Data subjects also have the right to withdraw consent and to have their personal data erased. As Sunderland college relies less on consent and more on 'contract' and 'legitimate interests' as a lawful basis for processing, subject requests will always be viewed in conjunction with the prevailing lawful bases.

Privacy Impact Assessment – a procedure by which each new system / activity undergoes a risk assessment to identify any potential risks to personal data, along with action planning of activities to mitigate risks.

4. RESPONSIBILITIES AND DUTIES

THE COLLEGE GOVERNORS AND SENIOR LEADERSHIP TEAM
It is the responsibility of the Board of Governors and the Senior Leadership Team to:

1. Ensure that the college has a nominated Data Protection Officer.

2. Ensure that appropriate systems and procedures exist in order to comply with Data Protection legislation. Procedures are listed in section 5.

3. Ensure that the college replaces current Data Protection Registration with the Information Commissioner's Office with Statutory ICO fee when current registration fee expires.

4. Ensure that the college provides all staff and students and other relevant users with information about the college's Data Protection Policy and Procedures, to be included in the College Charter, Staff and Student Handbook. The Policy can also be accessed electronically

Data Protection Officer

It is the responsibility of the Data Protection Officer (DPO) to:

1. Monitor data protection compliance against privacy rights, data protection law (including General Data Protection Regulations) and internal data protection policies, ensuring that compliance checking activities are undertaken regularly.

2. Report to the Senior Leadership Team and Audit Committee. biannually, regarding the organisation's' compliance with Data Protection Policy and Procedures.

3. Provide training and awareness-raising

4. Provide expert advice, guidance, and information to the organisation and those processing its data, regarding their legal obligations.

5. Provide advice and actively support the process of Privacy Impact Assessments, ensuring privacy by design is embedded into all college developments and reported regularly to the Resources and Infrastructure Committee.

6. Monitor and provide guidance as necessary in relation to data security breaches.

7. Liaise with data subjects and provide timely responses to requests.

8. Maintain appropriate records to enable the organisation to be able to demonstrate compliance with the law.

9. Cooperate and liaise with the supervisory authority for Data Protection.

STUDENTS

It is the responsibility of all students to:

1. Ensure that all personal data provided to the College is accurate and up to date.

2. Ensure that changes to personal data e.g. address or name, are notified to the student records data staff either via their teacher or directly.

EMPLOYEES

It is the responsibility of all college employees, including managers, to:

1. Check that any information that they provide to the College in connection with their employment is accurate and up to date.

2. Inform the College of any changes to information which they have provided, e.g. changes of address. The College cannot be held responsible for any errors in staff members' personal information resulting from the failure of members of staff to do this.

3. Ensure that any personal data they hold about students complies with the Data Protection Principles listed in section 2 of this policy and that the systems in which personal data is stored (relevant filing system) is notified to the college's Data Protection Officer for inclusion in the Information Asset Register. In particular, staff must ensure that such data is accurate, up-to-date, fair, securely stored and not excessive in relation to its purpose.

4. Ensure that 'sensitive data' (ie. that relating to the student's physical or mental health, sexual life, political or religious views, trade union membership, or ethnicity or race) is not held, except with the approval of the College's Data Protection Officer. Such processing must be in line with the college's lawful basis for processing The exception to this is when the member of staff is satisfied that the processing of such data is necessary because it is in the vital interests of the data subject.
5. Keep personal data confidential – it must not be accessed by or disclosed to any student, or other member of staff, unless for normal academic or pastoral purposes, without agreement from the Data Protection Officer, or in line with College policy. Staff should note that unauthorised access or disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Unauthorised access or disclosure by a staff member knowingly in breach of this policy could result in prosecution of the individual concerned.

6. Personal Data, in the form of spreadsheets, databases or any other electronic information source, which is about any individual (student or staff) and therefore within the scope of the data protection act, must NOT leave the college, either on email or on a portable device e.g. laptop, memory stick, CD, without being encrypted for the protection of personal data. This

includes data being emailed externally. Further information can be found in the college's IT Policy.

7. Check, prior to recording personal data, that the data to be recorded is fair, necessary, accurate, securely storable, and not 'sensitive'.

5. COLLEGE PROCEDURES LINKED TO THIS POLICY (list)

A number of college procedures exist to underpin the Data Protection / GDPR Principles in section 2 and to provide assurance that the college complies with Data Protection legislation. These include procedures relating to:-

5.1 Lawful basis for processing
5.2 Consent to process
5.3 Updating and accuracy of personal data
5.4 Notification and amendments to the Information Asset Register
5.5 Processing security
5.6 Privacy Impact Assessment
5.7 References
5.8 Examination marks
5.9 Statistical and historical research
5.10 Data subject rights and subject access requests
5.11 Electronic data and portable devices containing personal data
5.12 Data Sharing
5.13 Breach prevention, detection and notification
5.14 Retention of personal data
5.15 Destruction and disposal of personal data

6. HOW HAS IMPACT ASSESSMENT TAKEN PLACE

Please consult on this. Specialist staff (eg Learning Support, Student Support, Health & Safety Officer) can support with this. (What are the intended and unintended impacts of this policy on individuals and groups according to equality and diversity characteristics? These characteristics include: age, disability, gender re-assignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation. How is equality and diversity embedded within this policy? The impact assessment must consider safeguarding considerations and requirements.)

The requirement for the Data Subject to make data access request in writing may disadvantage some individuals. The procedure has, therefore, been amended in order to allow students or staff to make such requests by either personal representation, electronically or in writing.

First level information about Data Protection including Privacy Statements, whitch signpost to the full policy, are included in documents such as the student handbook and on the college website.