Data Protection Policy

Review

Formal Review Cycle	3 Yearly		
Latest Formal Review (date)	15/12/2020	Next Formal Review Due (date)	15/12/2023
Policy Owner	Head of Corporate Governance and Policy		
Policy Author	Christine Stretesky		

Approvals

Board of Corp Y/N	Y	Committee		Date Board approved	15/12/2020
ELT Y/N	Y	ELT date approved	26/11/2020	Additional committee	

Publication

Website Y/N	Y	Intranet Y/N	Y	Student VLE Y/N	Y	Other	

Change History

Version	Date Reviewed/ Revised	Description of Change	Reviewed by	Approved by
V2	October 2020	Introduces Information Asset Owners with specific responsibilities	C Stretesky	C Stretesky

Data Protection Policy

1. Policy Statement

1.1. This policy is a policy of the City of Sunderland College, trading as Education Partnership North East (which includes Sunderland College, Hartlepool Sixth Form College and Northumberland College). These colleges will be referred to as "the College" throughout this document.

1.2. As an organisation that collects, uses and stores Personal Data about its learners, employees, partners, suppliers, volunteers, parents and visitors, the College recognises that having controls around the collection, use, retention and destruction of Personal Data is important to comply with the College's obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

1.3. 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, marketing activity and non-government funded student activity.

1.4. The College understands it acts as data steward for the data it processes and is committed to compliance with the Data Protection Legislation, and specifically with General Data Protection Regulations (GDPR), ensuring that personal information is collected and used fairly, stored safely, and not disclosed to any other person or organisation unlawfully.

1.5. The Data Protection Registration Number for City of Sunderland College is Z7456751. The College's entry on the register can be viewed at https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/

2. Scope

2.1. This Policy applies to all parts of the City of Sunderland College ('the College'), as a single organisation ('Data Controller'). It is important to note, that while City of Sunderland College trades as four entities (Education Partnership NE, Sunderland College, Hartlepool Sixth Form and Northumberland College), it is a single legal entity and a single Data Controller.

2.2. This Policy applies to all staff acting in their official capacity as an employee of the College. In this policy, the term 'staff' means anyone working in any context within the College at whatever level or grade and whether permanent, fixed term or temporary, including but not limited to employees, workers, trainees, interns, seconded staff, agency staff, governors, and volunteers.

2.3. This Policy applies to all students and apprentices when processing Personal Data on behalf of the College or in relation to their Personal Data.

3. Aims of the Policy/Underpinning Principles

3.1. The College adopts the principles outlined within GDPR and has systems and processes in place to ensure compliance with these.

3.2. It is the aim of this Policy to ensure that Personal Data is:

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

3.2.2. 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.

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

3.2.4. 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.

3.2.5. 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.

3.2.6. 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.

3.3. The Lawful Bases upon which the College relies for its processing of Personal Data are primarily:

3.3.1. 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.
3.3.2. 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.
3.3.3. Public task: The processing is necessary for the College to carry out its official functions.
3.3.4. In some circumstances, consent may be requested from data subjects.

3.4. The College values diversity and inclusion and is committed to promoting equal opportunities and eliminating discrimination. Therefore, everyone will apply and administer this policy fairly and consistently to ensure that there is no discrimination on the grounds of age, disability, gender reassignment, marital and civil partnership status, pregnancy and maternity, race, religion or belief, sex, sexual orientation, persons in care and care leavers, carers and care givers, young parents, youth offenders, and those receiving free school meals.

4. Responsibilities

4.1. It is the responsibility of the Governors and the Executive Leadership Team to:

- Ensure that the College has a nominated Data Protection Officer (DPO)
- Ensure that appropriate systems and procedures exist in order to comply with Data Protection legislation. Procedures are listed in section 6
- Ensure that the College maintains registration with the Information Commissioner's Office
- Ensure that the College provides all staff and students and other relevant users with information about the College's Data Protection Policy and associated procedures, to be included in the College Charter, Staff and Student Handbook
- Ensure that the Information Asset Owners and DPO possess the necessary support, knowledge and skills to undertake their roles effectively

4.2. It is the responsibility of the Senior Information Asset Owner to act as data steward to:

- Be accountable to the College that Personal Data held within their business unit is processed in a manner consistent with this Policy
- Oversee the work of the Information Asset Owner within their business unit

4.3. It is the responsibility of the Information Asset Owner to act as data steward to:

- Lead and foster a culture that values, protects and uses Personal Data lawfully for the success of the organisation and benefit of our students and stakeholders
- Know what information comprises or is associated with the asset, and understand the nature and justification of information flows to and from the asset
- Know who has access to the asset and why, whether it be system or information to ensure access is monitored and compliant with policy
- Understand and address risks to the asset, and provide assurance to the Executive Leadership Team and Governors that risks are being addressed

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

- Monitor data protection compliance against privacy rights, data protection law (including General Data Protection Regulations) and internal data protection policies and procedures, ensuring that compliance checking activities are undertaken regularly
- Report to the Executive Leadership Team and Audit Committee annually, regarding the College's compliance with Data Protection Policy and Procedures
- Provide training and awareness-raising to staff
- Provide expert advice, guidance, and information to the College and those processing Personal Data regarding their legal obligations
- Provide advice and actively support the process of Data Protection Impact Assessments, ensuring privacy by design is embedded into all College developments
- Monitor and provide guidance as necessary in relation to data security breaches
- Liaise with data subjects and provide timely responses to requests
- Maintain appropriate records to enable the College to be able to demonstrate compliance with the law
- Cooperate and liaise with the supervisory authority for Data Protection

4.5. It is the responsibility of all students and apprentices to:

- Ensure that all Personal Data provided to the College is accurate and up to date
- 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

4.6. It is the responsibility of all College employees to:

- Check that any information that they provide to the College in connection with their employment is accurate and up to date
- 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
- Ensure that any Personal Data they hold about students complies with the Data Protection Principles listed in section 5 of this Policy and that the systems in which Personal Data is stored (relevant filing system) is notified to the Information Asset Owner 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
- Ensure that 'sensitive data' (ie. that relating to the Data Subject'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
- 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
- Comply with the College's IT Usage Policy
- Check, prior to recording Personal Data, that the data to be recorded is fair, necessary, accurate, securely storable, and not 'sensitive'

5. Implementation

5.1. The College is transparent about the purposes for which Personal Data is processed and has clearly articulated Privacy Notices, Information Asset Registers and Data Sharing Agreements and index.

5.2. The College embraces the concept of Privacy by Design and has systems in place to ensure that any new system / activity undergoes a Data Protection Impact Assessment (DPIA).

5.3. This Policy is implemented through a series of procedures as listed in Section 6 below. To meet the specific obligations of the Data Protection Act 2018 and the GDPR the College will:

5.3.1. With regard to processing Personal Data;

- Adopt transparent and easily accessible Privacy Statements
- Complete Data Protection Impact Assessments
- Ensure we only collect information that is necessary for our lawful purposes

- Detail information assets containing Personal Data in an Information Asset Register
- Ensure transparency through the use of robust Privacy Notices
- Ensure the accuracy of the Personal Data held through the use of easy systems for updating personal information
- Ensure we are keeping Personal Data only for as long as is necessary through compliance with a Data Retention and Destruction Schedule

5.3.2. With regard to data security; maintain appropriate technologies to maintain the security of all Personal Data from the point of collection to the point of destruction

5.3.3. With regard to the storing of data; ensure that Personal Data is not stored outside of the European Economic Area

5.3.4. With regard to data breach;
- Mitigate the risk of data breach through effective training and awareness raising to embed security and prevention practices into everyday practice
- Ensure appropriate procedures are in place to respond to any potential breach

5.3.5. With regard to subject access requests; ensure that appropriate procedures are in place so that data subjects are able to easily apply their individual rights under the GDPR

5.3.6. With regard to appointing contractor's with access to Personal Data;
- Conduct sufficient due diligence to ensure high standards with regard to data protection
- Require a written Data Sharing Agreement be in place

5.4. College employees will receive a copy of this Policy during induction and may receive periodic revisions of this Policy. This Policy does not form part of any contract of employment and the College reserves the right to change this Policy at any time.

5.5. This Policy will be maintained on the Education Partnership NE website and College intranet.

5.6. For more information about this Policy or data protection in general, please contact the Data Protection Officer at governance@educationpartnershipne.ac.uk

5.7. More information regarding data protection can also be found on the Information Commissioner's Office website: www.ico.org.uk

5.8. Key Terms

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

5.8.2. Data Controller - A data controller is an organisation that has full authority to decide how and why Personal Data is to be processed, and that has the overall responsibility for the data. This includes deciding on use, storage and deletion of the data.

5.8.3. Data Processor - A processor is responsible for processing Personal Data on behalf of a controller.

5.8.4. Data Subject – The subject of the data processed. A natural person who can be identified, directly or indirectly from data held.

5.8.5. Information Asset - An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.

5.8.6. Information Asset Owner - A member of senior leadership involved in running the relevant business units of the College. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why.

5.8.7. 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.

5.8.8. Processing - Processing is any action taken with Personal Data. This includes the collection, use, disclosure, destruction and holding of data.

5.8.9. 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.

5.8.10. 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, genetic data or biometric data.

5.8.11. Senior Information Asset Owner - A member of executive leadership with strategic responsibility over the relevant business units of the College. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why.

5.8.12. Data subject's 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 the 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.

5.8.13. Data Protection Impact Assessment – a procedure by which each modified or new system / activity undergoes a risk assessment to identify any potential risks to Personal Data, along with action planning of activities to mitigate risks.

6. Associated Documents

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:

- Lawful basis for processing

- Consent to process
- Updating and accuracy of Personal Data
- Notification and amendments to the Information Asset Register
- Processing security
- Privacy Impact Assessment
- References
- Examination marks
- Data subject rights and subject access requests
- Electronic data and portable devices containing Personal Data
- Data Sharing
- Breach prevention, detection and notification
- Retention, destruction and disposal of Personal Data

7. Policy Monitoring and Review

7.1. This Policy will be reviewed every three years or when legislative changes deem it necessary.

7.2. Information Asset Owners will undertake an annual audit to ensure compliance with this Policy and to ensure the Policy remains fit for purpose.

7.3. The Data Protection Officer will prepare an annual report for presentation to the ELT and Audit Committee providing assurance of compliance with this Policy, the Data Protection Act and GDPR.

8. Equality Impact Assessment

Have you sought consultation on this policy? **Details:**		Information Asset Owners Teams set up for comment and input into the policy		
Could a particular group be affected (negatively or positively)?	**Impact Y/N**	**Description of Impact**	**Evidence**	**Mitigation/ Justification**
Protected characteristics under the Equality Act 2010				
Age	N			
Disability	Y	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.

		Those with visual impairments may have trouble reading Privacy Statements		Privacy Statements to be made available in large print Website to meet the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018
Gender Reassignment	Y	College systems may not allow for inclusion of acquired gender or preferred name		Our student ILR is a system we are required to use by the ESFA and therefore cannot modify Where we are able, the College will use the acquired gender and preferred name of data subjects and will maintain appropriate records
Marriage and Civil Partnership	N			
Pregnancy and maternity	N			
Race	N			
Religion or belief	N			
Sex	N			
Sexual Orientation	N			
Additional characteristics to consider				
Young Persons in Care & Care Leavers	N			
Young Carers & Care Givers	N			
Young Parents	N			

Youth Offenders	N			
Those Receiving Free School Meals	N			
If there is no impact, please explain:				