Data Protection Policy

Ref QA42

Data Protection Policy

Review Date: June 2020

The Policy

North East Scotland College (NESCol) has a wide range of educational and business requirements to maintain personal data so that our activities as a further education college can be delivered. We create, gather, store and process large amounts of data on a variety of data subjects (people) including students (potential, current and former), staff, customers/suppliers and members of the public.

The college must comply with the EU General Data Protection Regulation, the Data Protection Act 2018 and other relevant legislation. These laws require the college to protect personal information and control how it is used in accordance with the legal rights of the data subjects – the people whose personal information is held.

There are obligations on the college regarding the way it handles personal data and in turn, college staff and students have responsibilities to ensure personal data is processed fairly, lawfully and transparently. This means that personal data should only be processed if we have a valid condition of processing and we have provided information to the individuals concerned about how and why we are processing their data (i.e. a privacy notice). There are restrictions on what we are allowed to do with personal data such as passing it to third parties, transferring it outside the EU or using it for direct marketing.

Scope of policy

1. This policy applies to all Board members, staff, students, contractors and partners working on behalf of the college.

2. The policy applies to all personal data created, collected, stored, adapted, transferred, erased, destroyed and otherwise processed through any activity of NESCol. Personal data may be held or shared in paper and electronic formats or communicated verbally in conversation or by phone.

3. The policy also applies to all locations from which college personal data is accessed, including home use.

Definitions

Personal data: any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. An identifier may be name, an identification number, location data, an

online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data subject: the living individual to whom the personal data relates. This includes, but is not limited to: prospective applicants, current and former students, current and former employees, visiting students and staff, family members where emergency and next of kin contacts are held, Board members, volunteers, event delegates.

Data controller: any person, public authority, agency or other body who determines the purposes for which and the way in which any personal data is to be processed. For the purposes of this policy, North East Scotland College (NESCol) is the data controller and is registered with the Office of the Information Commissioner.

Processing: any operation or set of operations performed on personal data such as collection, organising, storing, adapting, retrieving, transmitting, erasing or destroying.

Subject access request: a request for a copy of one's own personal data

Data Protection Officer: the member of staff with oversight of organisational and technical measures and controls to comply with the data protection legislation

Responsibilities

1. All users of college information (students, staff and other users) are responsible for:
    a. completing relevant training and awareness activities provided by the college to support compliance with the Data Protection policy and relevant procedures
    b. taking all necessary steps to ensure that no breaches of information security result from their actions
    c. reporting all suspected information security (data) breaches or incidents promptly so that appropriate action can be taken to minimise harm
    d. Informing the college of any changes to the information that they have provided to the college in connection with their studies or employment, for instance, changes of address or bank account details.
2. The Principal of North East Scotland College has ultimate accountability for the college's compliance with data protection law and for ensuring that the Data Protection Officer is given sufficient autonomy and resources to carry out their tasks effectively.

3. The Vice Principal – Access and Partnerships is responsible for acting as the contact for the Senior Management Team and will ensure that students comply with Data Protection legislation.
4. The Director of Student Access and Support is responsible for information governance and will act as the contact for the Leadership Team.
5. The Data Protection Officer is responsible for:
    a. informing and advising senior managers and all members of the college community of their obligations under data protection law
    b. promoting a culture of data protection, e.g. through training and awareness activities
    c. reviewing and recommending policies, procedures, standards, and controls to maintain and demonstrate compliance with data protection law and embed privacy by design and default across the college
    d. advising on data protection impact assessment and monitoring its performance
    e. monitoring and reporting on compliance to the Senior Management Team, the Regional Board and committees as appropriate
    f. ensuring that Records of Processing and 3rd party sharing activities are maintained
    g. providing a point of contact for data subjects with regard to all issues related to their rights under data protection law
    h. investigating personal data breaches, recommending actions to reduce their impact and likelihood of recurrence
    i. acting as the contact point for and cooperating with the Information Commissioner's Office on issues relating to processing;

    Where permissible under the legislation, some of these duties may also be undertaken by the Director of Student Access and Support, or other arrangements may be made for oversight of these duties.
6. All team managers are responsible for implementing this policy within their business areas and for adherence by staff. This includes:
    a. assigning generic and specific responsibilities for data protection management
    b. managing access rights for information assets and systems to ensure that staff, contractors and agents have access only to such personal data is necessary for them to fulfil their duties
    c. ensuring that all staff in their areas of responsibility undertake relevant and appropriate training and are aware of their responsibilities for data protection
    d. ensuring that staff responsible for any locally managed IT services liaise with college's IT staff to put in place equivalent IT security controls
    e. assisting the Data Protection Officer in maintaining accurate

and up to date records of data processing activities

f. ensuring that they and their staff cooperate and support the Data Protection Officer in relation to subject access requests and other requests relating to personal data where the data is managed by their business area; and
g. recording data protection and information security risks on the Operational Risk Register and escalating these as necessary.

7. The Director of HR and OD will ensure that staff roles and responsibilities are clearly defined in terms of data protection and that Job Descriptions and Person Specifications reflect this.
8. The Director of Information Technology is responsible for:
    a. ensuring that centrally managed IT systems and services are embed by privacy by design and default;
    b. promoting good practice in IT security among staff; and
    c. ensuring, in conjunction with the Data Protection Officer, that IT security risks related to data protection are captured on the college risk registers.

Policy statement

The college is committed to applying the principles of data protection to the management of personal data at all stages of its lifecycle. The following policy objectives will be adopted:

We will process data fairly and lawfully

This means we will

- only collect personal information where it is necessary so that we can deliver our functions and services.
- ensure that if we collect personal data for a specific purpose, or purposes, we will not reuse it for a different purpose that the individual did not agree to or expect
- rely on consent as a condition for processing only where we obtain specific, informed and freely given consent that is affirmative and documented.

We will tell data subjects what is done with their personal data

As we collect personal data we will explain, in simple terms:

- What we collect and what we use it for
- the lawful basis we rely on to process the data (for each purpose)
- Whether we use it for any other legitimate purpose
- Whether the data is needed to meet a statutory or contractual requirement
- The source of the data, including where we receive it from third parties
- Whether we use automated decision making or profiling

- How we will protect the data
- Who we may disclose it to
- How long we keep the data for and how we dispose of it when no longer required
- How data subjects can update the personal data we hold
- How data subjects can exercise their rights
- Who our Data Protection Officer is and how they can be contacted

Privacy notices

The college will use privacy notices to let data subjects know what is done with their personal data.

Privacy notices are published on the college website and are available to staff and students from their first point of contact with the college.

Any processing of staff or student data beyond the scope of the standard privacy notices will mean that a separate privacy notice is required.

We will regularly review these privacy notices and will inform the relevant data subjects of any changes that may affect them.

Data subject rights and subject access requests

NESCol will uphold a data subject's rights to:

- obtain a copy of the information comprising their personal data (known as making a subject access request)
- have inaccurate personal data rectified and incomplete personal data completed
- have their personal data erased when it is no longer needed, if the data have been unlawfully processed or if the data subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data
- restrict the processing of their personal data until a dispute about the data's accuracy or use has been resolved, or when the college no longer needs to keep personal data but the data subject needs the data for a legal claim
- data portability (if applicable): where a data subject has provided personal data to the college by consent or contract for automated processing and asks for a machine readable copy or to have the data sent to another data controller
- object to and prevent further processing of their data for the legitimate interests or public interest unless the college can demonstrate compelling lawful grounds for continuing

- prevent processing of their data for direct marketing
- object to decisions that affect them being taken solely by automated means (if applicable); and
- claim compensation for damages caused by a breach of data protection law.

Subject access requests (requests for a copy of one's own personal data) will be responded to by the college, free of charge, within one month of the request being received. A further two months to respond may be granted in exceptional circumstances, for example if the request is complex or a number of requests are received from the same person.

NESCol will also ensure it communicates to all data subjects their right to lodge a complaint with the Information Commissioner's Office.

Data retention and security

NESCol has a records management policy which applies to all records created, received or maintained by college staff in the course of carrying out their duties (with the exception of student assessment material which is covered by the Assessment and Verification Policy). It provides the framework for the college's approach to records management, including the full lifecycle of records.

The retention and security of personal data is part of this wider framework and personal data records will be managed in line with the requirements of the records management policy.

The college also sets and monitors security standards for the management of personal data as part of the college's information security framework. The Information Systems Security Policy outlines the steps that must be taken to prevent unauthorised access to college confidential information; and outlines unacceptable use, which has a direct impact on risks associated with personal data.

Data breaches

NESCol will take all necessary steps to reduce the likelihood of data breaches and to reduce the impact of any incidents involving personal data that do occur.

All data breaches will be reported to the Data Protection Officer in the first instance. If a breach is likely to result in a risk to the rights and freedoms of a data subject, the Data Protection Officer will liaise with the Information Commissioner's Office within 72 hours of discovery (in line with regulatory requirements).

NESCol is committed to a culture which encourages early identification of data protection incidents and which provides appropriate training and support to individuals involved. Notwithstanding this, the college will, where deliberate or wilful behaviour leads to a data protection incident, take appropriate disciplinary action and/or report the matter to the police, in line with relevant HR policies.

We will also identify 'near misses' where an unplanned event did not lead to a data protection breach but had the potential to. We will use these events as 'learning points' as part of the continual improvement of our data handling processes.

Relationship with other policies

This policy has been formulated within the context of the following College documents:

1. Records Management Policy
2. Information Systems Security Policy
3. Freedom of Information Policy
4. Acceptable Use Policy – internet and email – students
5. Acceptable Use Policy – internet and email – staff

Status:	Approved
Approved By:	Principal
Date of Version:	20 June 2018
Responsibility for Policy:	Director of Student Access and Support
Responsibility for Implementation:	Director of Student Access and Support, Data Protection Officer
Responsibility for Review:	Director of Student Access and Support
Review Date:	June 2020
EIA Date:	20 June 2018

Equality Impact Assessment (EIA) Form

Part 1. Background Information. (Please enter relevant information as specified.)

Title of Policy or Procedure. Details of Relevant Practice:	Data Protection Policy
Person(s) Responsible.	Director of Student Access and Support
Date of Assessment:	
What are the aims of the policy, procedure or practice being considered?	The aim of the policy is to set out how North East Scotland College will comply with the General Data Protection Regulation.
Who will this policy, procedure or practice impact upon?	This will impact on applicants, students, staff, contractors and members of the public.

Part 2. Public Sector Equality Duty comparison (Consider the proposed action against each element of the PSED and describe potential impact, which may be positive, neutral or negative. Provide details of evidence.)

Need	Impact	Evidence
• **Eliminating unlawful discrimination, harassment and victimisation.**	Positive	This policy will have a positive impact on those with protected characteristics by providing a framework within which special categories of data (sensitive data) will only be processed (including shared) when the specific conditions are met.
• **Advancing Equality of Opportunity**	Neutral	This policy will have no impact on those with protected characteristics with regards to advancing opportunities.
• **Promoting Good relations**	Positive	This policy will have a positive impact on those with protected characteristics by providing a framework within which special categories of data will be managed fairly, lawfully and securely.

Part 3. Action & Outcome (Following initial assessment, describe any action that will be taken to address impact detected)

Sign-off, authorisation and publishing *	
Name:	Jacqueline Gillanders
Position:	Data Protection Officer
Date of original EIA	
Date EIA last reviewed	20 June 2018

**Please note that an electronic sign-off is sufficient*

