Policy/Procedure/Guideline Review

Policy/Procedure/ Guideline:	Data Protection Policy
Senior Manager Responsible:	Data Protection Officer
Author:	Admin Services Manager
Approved By:	Board of Corporation
Date Approved:	1 October 2018
Next Review Date:	October 2019
Publication:	Nelson and Colne College's Extranet Nelson and Colne College and Lancashire Adult Learning Websites
Changes Made:	Updated policy to ensure compliance with GDPR requirements. Dec 18 – Updated to include Accrington and Rossendale College

Data Protection Policy

1. Introduction

1.1 Nelson and Colne College including Lancashire Adult Learning and Accrington and Rossendale College ('the College') is committed to protecting the confidentiality and integrity of Personal Data and this is a key responsibility of everyone within the College.

1.2 As an organisation that collects, uses and stores Personal Data about its employees, suppliers (sole traders, partnerships or individuals within companies), students, governors, parents and visitors the College recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order 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 has implemented this Data Protection Policy to ensure all staff are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and will provide for a successful working and learning environment for all.

1.4 Queries concerning this policy should be directed to the Data Protection Officer (DPO).

2. Scope

2.1 This policy (and the other policies and documents referred to in it) sets out the basis on which the College will collect and use Personal Data either where the College collects it from individuals itself, or where it is provided to the College by third parties. It also sets out rules on how the College handles, uses, transfers and stores Personal Data.

2.2 It applies to all Personal Data stored electronically, in paper form, or otherwise.

3. Definitions

3.1 **College** – Nelson and Colne College including Lancashire Adult Learning and Accrington and Rossendale College.

3.2 **Staff** – Any College employee or contractor who has been authorised to access any of our Personal Data and will include employees, consultants, contractors, and temporary staff hired to work on behalf of the College.

3.3 **Controller** – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data. A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the College is the Controller of include employee details. The

College will be viewed as a Controller of Personal Data if it decides what Personal Data is going to be collected and how it will be used.

3.4 **Processor** – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller. A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data, e.g. where software support for a system, which contains Personal Data, is provided by someone outside the organisation; cloud arrangements; and mail fulfilment services.

3.5 **Data Protection Laws** – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

3.6 **Data Protection Officer (DPO) –** The Data Protection Officer is Leanne Powell and can be contacted on 01282 440200 or via email DPO@nelson.ac.uk or DPO@accross.ac.uk

3.7 **College Leadership Team (CLT)** – Responsible for data protection within their areas and providing support to the DPO.

3.8 **EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

3.9 **ICO** – Information Commissioner's Office, the UK's data protection regulator.

3.10 **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location, if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

3.11 **Personal Data** – Any information about an individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context. Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of individuals in companies such as firstname.surname@organisation.com, IP address and also more sensitive types of data (see Special Categories of Personal Data below).

3.12 **Special Categories of Personal Data** – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical

beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are given extra protection by Data Protection Laws and as such are subject to additional controls in comparison to ordinary Personal Data.

3.13 **Automated Decision Making** happens where the College makes a decision about an individual solely by automated means without any human involvement and the decision has legal or other significant effects.

3.14 **Profiling** happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

3.15 **Information Asset Register (IAR)** – the College's mechanism for recording and managing information assets and the risks to them; including the links between the information assets, their business requirements and technical dependencies.

4. Staff Responsibilities

4.1 All staff must comply with this policy at all times.

4.2 Staff must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

4.3 Staff must not release or disclose any Personal Data outside the College or inside the College to staff not authorised to access the Personal Data, without specific authorisation from their Manager or the Data Protection Officer. This includes by phone calls or in emails.

4.4 Staff must take all steps to ensure there is no unauthorised access to Personal Data whether by other College Staff who are not authorised to see such Personal Data or by individuals outside the College.

4.5 If staff intend to change how they use Personal Data, the Data Protection Officer must be notified who will, in conjunction with the appropriate College Leadership Team member, decide whether the intended use requires amendments to be made to the lawful basis, privacy notices and any other controls which need to apply. The College Information Asset Register (IAR) must also be updated.

4.6 Staff that access Personal Data must review and update it as necessary to ensure its accuracy is maintained (see section 8.4).

5. Data Protection Principles

5.1 When using Personal Data, Data Protection Laws (Article 5 of the GDPR) require that the College complies with the following principles. These principles require Personal Data to be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
- kept for no longer than is necessary for the purposes for which it is being processed; and
- 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.

5.2 These principles are considered in more detail in the remainder of this Policy.

5.3 In addition to complying with the above requirements the College also has to demonstrate in writing that it complies with them. The College has a number of policies and procedures in place, including this policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance.

6. Lawful Use of Personal Data

6.1 In order to collect and/or use Personal Data lawfully the College needs to be able to show that its use meets one of a number of legal grounds. The grounds are detailed on the ICO website (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing).

6.2 In addition when the College collects and/or uses Special Categories of Personal Data, the College has to show that one of a number of additional conditions is met. The additional conditions are detailed on the ICO website (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data).

6.3 The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in section 5. If the College changes how it uses Personal Data, the College information asset register (IAR) will be

updated and individual(s) may need to be notified about the change. Intended changes must be notified to the Data Protection Officer to determine whether their intended use requires amendments to be made and any other controls which need to apply. This would be determined in conjunction with the appropriate member of the College Leadership Team.

7. Transparent Processing – Privacy Notices

7.1 Where the College collects Personal Data directly from individuals, they will be informed in a privacy notice about how the College uses their Personal Data. The College privacy notices can be found on the College website.

7.2 If the College receives Personal Data about an individual from other sources, a privacy notice will be provided to the individual about how the College will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

7.3 If the College changes how it uses Personal Data, individuals may need to be notified about the change. If staff therefore intend to change how they use Personal Data the Data Protection Officer must be notified who will, in conjunction with the appropriate member of the College Leadership Team, decide whether the intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

8. Data Quality – Ensuring the Use of Accurate, Up to Date and Relevant Personal Data

8.1 Data Protection Laws require that the College only collects and processes Personal Data to the extent that it is required for the specific purpose(s), notified to the individual in a privacy notice. The College is also required to ensure that the Personal Data it holds is accurate and kept up to date.

8.2 All staff that collect and record Personal Data (including from sources outside of the College) shall ensure that the Personal Data is:

- recorded accurately;
- kept up to date;
- limit the collection and recording to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

8.3 Personal Data from sources outside the College does not require staff to independently check the Personal Data obtained.

8.4 In order to maintain the quality of Personal Data, all staff that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not apply to Personal Data which the College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

8.5 The College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The College has a Rights of Individuals Policy and Procedure which set out how the College responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with this policy and procedure.

9. Personal Data Must not be Kept for Longer than Needed

9.1 Data Protection Laws require that the College does not keep Personal Data longer than is necessary for the purpose or purposes for which the College collected it.

9.2 The College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the College, the reasons for those retention periods and how the College securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.

9.3 If staff consider that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if staff have any questions about this Policy or the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

10. Data Security

10.1 The College takes information security very seriously and has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

11. Data Breach

11.1 Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and staff must comply with the Data Breach Notification Policy.

11.2 Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

11.3 There are three main types of Personal Data breach which are as follows:

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a member of staff is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;

- **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

- **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

12. Appointing Contractors who access the College's Personal Data

12.1 If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where sufficient due diligence has been carried out and only where appropriate contracts are in place.

12.2 One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. To meet this requirement data protection due diligence is undertaken on both new and existing suppliers. Once a Processor is appointed they will be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

12.3 All contracts where the College appoints a Processor will be in writing.

12.4 A Processor is considered appointed where someone is engaged to perform a service for College and as part of it they may get access to College Personal Data. College remains the Controller of the data and therefore responsible for what happens to the Personal Data.

12.5 In accordance with GDPR the College requires the contract with a Processor to contain the following obligations as a minimum:

- to only act on the written instructions of the Controller;

- to not export Personal Data without the Controller's instruction;

- to ensure staff are subject to confidentiality obligations;

- to take appropriate security measures;

- to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;

- to keep the Personal Data secure and assist the Controller to do so;
- to assist with the notification of Data Breaches and Data Protection Impact Assessments;

- to assist with subject access/individuals rights;

- to delete/return all Personal Data as requested at the end of the contract;

- to submit to audits and provide information about the processing; and

- to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

12.6 In addition the contract should set out:

- The subject-matter and duration of the processing;

- the nature and purpose of the processing;

- the type of Personal Data and categories of individuals; and

- the obligations and rights of the Controller.

13. Individual's Rights

13.1 GDPR gives individuals more control about how their data is collected and stored and what is done with it. The different types of rights of individuals are stated below:

Subject Access Requests (SAR)

13.1.1 Individuals have the right under the GDPR to ask the College to confirm what Personal Data they hold in relation to them and provide them with the data. The timescale for providing the information is one month (with a possible extension if it is a complex request). Fees will not be charged for complying with the request.

Right of Erasure (Right to be Forgotten)

13.1.2 This is a limited right for individuals to request the erasure of Personal Data concerning them where:

- the use of the Personal Data is no longer necessary;

- their consent is withdrawn and there is no other legal ground for the processing;

- the individual objects to the processing and there are no overriding legitimate grounds for the processing;

- the Personal Data has been unlawfully processed; and

- the Personal Data has to be erased for compliance with a legal obligation.

13.1.3 In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

Right of Data Portability

13.1.4 An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine readable format where:

- the processing is based on consent or on a contract; and

- the processing is carried out by automated means

- This right isn't the same as subject access and is intended to give individuals a subset of their data.

The Right of Rectification and Restriction

13.1.5 Finally, individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

13.1.6 The College will use all Personal Data in accordance with the rights given to individuals' under Data Protection Laws, and will ensure that it allows individuals to exercise their rights in accordance with the College's GDPR - Rights of Individuals Policy.

14. Marketing and Consent

14.1 The College will sometimes contact individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

14.2 Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR has brought about a number important changes and as a result the College will:

- provide more detail in privacy notices, including for example whether profiling takes place; and

- obtain consent via an individual's "clear affirmative action", namely an unticked opt in box.

14.3 Alternatively, where a “soft opt in” is appropriate this will be used but only where the following conditions are met:

- contact details have been obtained in the course of a sale (or negotiations for a sale);
- the College are marketing its own similar services; and
- the College gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

14.4 The Privacy and Electronic Communications Regulations (PECR) sit alongside data protection. PECR apply to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails and texts. PECR rules apply even if you are not processing any personal data.

15. Automated Decision Making and Profiling

15.1 Under Data Protection Laws there are controls around profiling and automated decision making in relation to individuals.

15.2 If staff wish to carry out any Automated Decision Making or Profiling the Data Protection Officer must be informed and approval provided before commencement.

15.3 The College does not carry out Automated Decision Making or Profiling in relation to its employees.

16. Data Protection Impact Assessments (DPIA)

16.1 The GDPR introduces a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (DPIA). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and
- the measures to address the risks.

16.2 A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals.

16.3 Where a DPIA reveals risks which are not appropriately mitigated the Data Protection Officer must be informed as the ICO must be consulted.

16.4 Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, it needs to be considered whether a DPIA needs to be carried out as part of the project initiation process. A DPIA must be carried out at an early stage in the process so that the problems can be identified and fixed with the proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

16.5 Situations where a DPIA may need to be carried out include the following (please note that this list is not exhaustive):

- large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;

- large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or

- systematic monitoring of public areas on a large scale e.g. CCTV cameras.

16.6 All DPIAs must be reviewed and approved by the Data Protection Officer and the appropriate member of the College Leadership Team.

17. Transferring Personal Data to a County Outside the EEA

17.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. Appointments of suppliers or suppliers with group companies outside the EEA need to be carefully considered where access to the Personal Data to staff outside the EEA maybe given.

17.2 To ensure compliance with Data Protection Laws staff must not export Personal Data unless it has been approved by the appropriate member of the College Leadership Team.

17.3 Staff must not export any Personal Data outside the EEA without the approval of the Data Protection Officer and the appropriate member of the College Leadership Team.

18. Dissemination

18.1 A copy of this policy and procedure can be found on:

- Nelson and Colne College's Extranet
- Accrington and Rossendale College Intranet
- Nelson and Colne College, Lancashire Adult Learning and Accrington and Rossendale Websites

19. Monitoring and Review

19.1 The policy and operation of the procedure will be monitored and reviewed by Nelson and Colne College's Data Protection Officer.

19.2 The College reserves the right to change this policy at any time.

20. Related Policies and Procedures

20.1 Documents related to this policy are:

- Rights of Individuals Policy
- Data Breach Notification Procedure
- Data Retention Policy
- Freedom of Information Procedure
- Subject Access Request Procedure

21. Management Responsibility

21.1 The Data Protection Officer has management responsibility for this policy across Nelson and Colne College.