New College Durham

Policy on

Data Protection

New College Durham is committed to safeguarding & promoting the welfare of children and young people, as well as vulnerable adults, and expects all staff and volunteers to share this commitment.

New College Durham

Data Protection Policy

(Equality and Diversity Assessment)

We will consider any request for this procedure to be made available in an alternative format.

We review our policies and procedures regularly to update them and to ensure that they are accessible and fair to all. All policies and procedures are subject to equality impact assessments. Equality Impact Assessments are carried out to see whether the policy has, or is likely to have, a different impact on grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation or human rights.

We are always keen to hear from anyone who wants to contribute to these impact assessments and we welcome suggestions for improving the accessibility or fairness of the policy.

To make suggestions, seek further information or if any employee has difficulty understanding this policy please contact the Information and Records Team at records@newdur.ac.uk

Equality Impact Assessed: August 2017

Procedure Title	**Data Protection Policy**
Document Owner	**Information, Records and Projects Manager**
Owning Directorate	**Corporate Services**
Owning Department	**ICT**

Directorates and Departments affected by this Procedure	**All staff**
Procedure Effective From	**September 2017**
Next Review Date	**September 2022**

Contents **Page**

New College Durham

Data Protection Policy

1. Scope

This Policy will enable compliance with relevant Data Protection Legislation and will be relevant to all College staff and outsourced service providers operating under data processing contracts or agreements with the College.

This Policy applies to all the information the College holds in any format.

Definitions of terms and the designation of articles referenced in this policy should be obtained from the GDPR Articles published by the EU[1].

This Policy will form part of the College's 'record of processing activities'.

2. Role definitions

New College Durham is the Data Controller for all personal data held in its systems as described in the Information Asset Register and the College Fileplan.

The Deputy Principal (Human Resources & Corporate Services) is the Senior Information Risk Owner (SIRO) for New College Durham.

The Information, Records and Projects Manager is the Data Protection Officer (DPO) for New College Durham.

A Data Owner is the person who holds managerial and financial accountability for a data set and determines its purposes and means of processing.

3. Responsibilities

The Corporation of New College Durham is responsible for ensuring the College has a Data Protection Policy.

The SIRO is responsible for authorising and requiring action in relation to data protection processes and procedures, risk and privacy assessments and the resourcing of staff training.

The Data Protection Officer will keep the register of processing activities and inform, advise and recommend in relation to data protection; having due regard for the risks associated with processing personal data.

[1] See https://gdpr-info.eu/

In addition the Data Protection Officer will:

- be easily accessible, with all staff made aware of the role;
- have the necessary level of expert knowledge;
- have sound knowledge of College rules and procedures;
- not hold a position where she or he determines the purposes or means of processing personal data;
- foster a data protection culture and implement essential elements of the law;
- be involved in all issues relating to the protection of personal data;
- advise on all Privacy Impact Assessments made by the College;
- be consulted on any data breach incident;
- given the resources and training necessary to fulfil DPO duties;
- act independently and not be instructed or influenced;
- not be penalised for performing tasks required by the role as set out in the legislation and working party guidance.

The Information, Records and Projects Manager is responsible for the provision of guidance in relation to this policy.

Data Owners are responsible for ensuring processing is done in compliance with this policy and the law.

Staff who have responsibility for the processing (ie. the collection, use, storage and retention) of any personal data are responsible for ensuring their processing is done in compliance with this policy and the law.

All staff are responsible for

- familiarising themselves with this policy;
- complying with a request for information from the Information, Records and Projects Manager/Data Protection Officer; and
- informing the Data Protection Officer if a communication is received from the Information Commissioner's Office.

Compliance with this Policy is compulsory for all staff employed by the College. A member of staff who fails to comply with the Policy may be subjected to action under the College's disciplinary policy or competence procedure. It is the responsibility of Heads of Departments/School and their Directors/Vice Principals to ensure that their staff are made aware of the existence of this Policy and its content.

4. Relationship with existing policies and legislation

This policy will facilitate compliance with the following legislation and guidance:

- General Data Protection Regulation[2]

[2] References to 'articles' throughout will refer to the text of the GDPR as published by the EU. This will also be construed to mean the UKGDPR if enacted.

- Data Protection Act 2018
- Privacy and Electronics Communications Regulations 2003 (and any successor legislation)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Article 29 Working Party Guidance

This Policy has been formulated within the context of the following College policies and documents which comprise its record of processing activities and should be made available to the Information Commissioner for Inspection.

- Records Management Policy
- Information Security Policy
- Management and Monitoring of Electronic Communications, Internet and Telephones Policy
- Information Asset Register
- Fileplan with RRS

- Guidance Note 1: Making a DP Request
- Guidance Note 2: Data Protection for Staff
- Guidance Note 3: Providing References
- Guidance Note 4: Code of Conduct for Photographs and Recordings
- Guidance Note 5: Use of Online Survey Software
- Guidance Note 6: Conducting a Data Protection Impact Assessment
- Guidance Note 7: Creating Privacy Notices
- Guidance Note 8: Legitimate Interests Assessment Form

5. Data Protection Principles

a. **Lawfulness, fairness and transparency**
To ensure that personal data is processed lawfully, the College will not process personal data unless one of the conditions of processing in article 6 is met or article 9 where relevant to the processing of special category data.

Where consent is used as the condition for processing then the conditions in article 7 and 8 will be met.

The conditions for processing special category data will be documented in the Fileplan.

b. **Purpose limitation**
The College will ensure that all processing of personal data is undertaken for specific, explicit and legitimate purposes and that the data is not further processed in a manner that is incompatible with those purposes.

c. **Data minimisation**
The College will ensure that personal data processed is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d. **Accuracy**
The College will ensure there are mechanisms to ensure personal data remains accurate and up to date.

e. **Storage limitation**
The College will ensure that personal data is processed no longer than necessary. The details of retention schedules will be held in the Fileplan and RRS.

f. **Integrity and confidentiality**
The College will ensure that personal data is processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing, accidental loss, destruction or damage using appropriate technical measures. The detail of these measures will be held in the Information Security Policy.

6. Data Subject Rights

a. Information and Access

The College will ensure all communications in relation to processing are done in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Privacy Notices will be provided to cover all instances of processing and will provide enough information to ensure compliance with article 13 of the GDPR.

Requests for access to personal data in relation to data subject rights will usually be managed by the Information, Records and Projects Manager, except for the following cases;

- requests for access to staff personal or occupational health files will be managed by the HR department; and
- requests for access to personal data in relation to data sharing arrangements will be managed by the member of staff named in the agreement.

b. Rectification and erasure

The College recognises the right of users to request rectification and erasure of their data in specific circumstances according to Articles 16, 17 and 19 of the GDPR.

Routine requests for amendments to personal data will be managed by the department responsible for processing the data.

Non-routine requests for rectification and erasure in relation to personal data will be identified by the department processing the data and referred to the Information, Records and Projects Manager, all requests will be managed with due regard to the relevant Articles of the GDPR.

c. Objection and Restriction

The College recognises the right of users to object to the processing of their data in certain circumstances according to Article 21 of the GDPR.

The College recognises the right of users to request that the processing of their data be restricted in specific circumstances according to Articles 18-19 of the GDPR.

All objections or requests for processing to be restricted will be managed by will be identified by the department processing the data and referred to the Information, Records and Projects Manager, all requests will be managed with due regard to the relevant Articles of the GDPR.

d. Portability

Where the College already holds data in machine readable format a requester may request a copy in the same format.

e. Automated processing

The College does not carry out automated processing as a matter of course. If a data subject is to be subject to automated processing as a result of participation in an ad-hoc project then they will be informed as part of the Privacy Notice for that project about the nature of the processing and their rights in relation to it.

7. Controller / Processor Responsibilities

Where New College Durham is designated a Processor by a contractual relationship it will still fulfil its duties under law regarding the security and integrity of the data held and act according to the contract terms.

Where the College identifies that a third party is a Processor on behalf of the College the Processor must be contractually bound using the College's standard Processor terms.

Where the College intends to designate a third party as a Processor in a contractual relationship or in a situation where the contract is the 'Terms and Conditions' of purchase, the College must require the third party to have

adequate security measures in place and, with reference to the Information Security Policy, this judgement will be made by the ICT Operations Manager.

Where data is held externally or 'hosted' by a third party, the third party is deemed to be a Processor and the requisite contractual obligation should be placed upon them unless they have already undertaken equivalent obligations in their standard terms and conditions.

The Data Owner / department owning the data which is to be processed, shared or hosted will be responsible for ensuring the relevant contractual terms are in place.

The Data Protection Officer should be asked to review any contract or terms and conditions to ensure the contractual obligation is robust.

8. Data Sharing Agreements

Data sharing between a Controller and Processor must be covered by a contract. This contract may be part of the terms and conditions of purchase in relation to hosted data services but will always need to define the Controller/Processor relationship.

Data sharing between two Controllers should be covered by a Data Sharing Agreement.

A Data Sharing Agreement may be a schedule included as part of a contract or a separate document. It will describe the process for sharing data, including the legal basis for the sharing and processing.

The department owning the data which is to be shared will be responsible for ensuring the relevant contractual terms are in place and adhered to.

The Data Protection Officer should be asked to review any data sharing agreement or relevant contract schedule to ensure the legal basis for processing is robust.

In cases where a third party organisation needs access to a College system containing personal data an agreement will be put in place.

The Data Protection Officer will maintain a list of relevant agreements and contract clauses.

Please refer to the flowchart at Appendix A: How to share data with a Third Party.

9. Data Breaches

Data breach incidents will be reported via the ICT helpdesk, as described in the Information Security Policy.

The Data Protection Officer will log the breaches and issue recommendations taking into account mitigation already applied directly to the ICT department and the SIRO. In line with legislation, the recommendations should be acted upon within 72 hours of the breach being reported.

Where the Data Protection Officer recommends that the breach is reportable to the Information Commissioner, the SIRO must be informed.

10. Data Protection Impact Assessments

Where a new system is implemented in which personal data will be processed, a Data Protection Impact Assessment must take place.

A Data Protection Impact Assessment should be conducted by the Data Owner for the personal data concerned.

Data Protection Impact Assessments must be reviewed by the Data Protection Officer. This should be done as part of the implementation plan for a new system.

The Data Protection Officer should provide written advice on any action required to ensure the processing of data in the new system is lawful and the ICT Operations Manager should be asked to advise on any areas of best practice in relation to Information Security.

If the Data Owner does not intend to implement the recommendations of the Data Protection Officer then the SIRO must be informed so that the College risk register can be updated.

11. Data Transfers

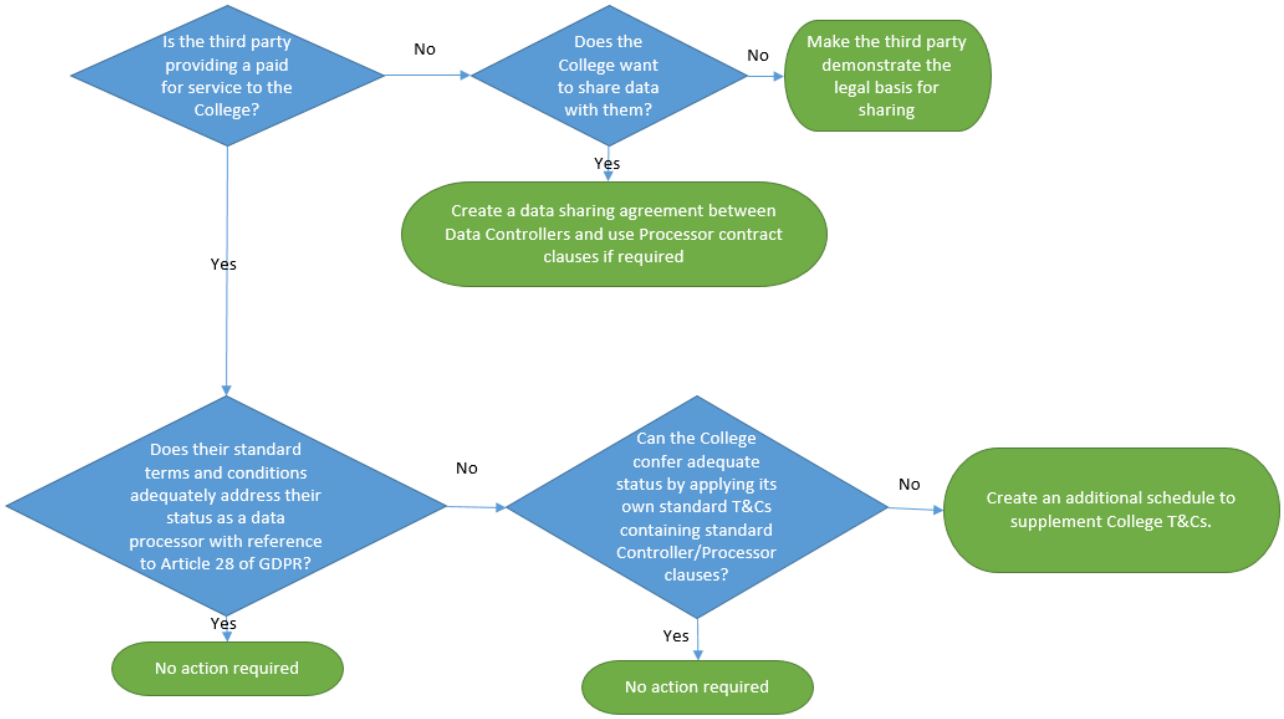
The mechanism for any processing of personal data for which the College is the Data Controller which takes place outside of the UK must be reviewed by the Data Protection Officer. This will usually occur under contract as per section 7 of this policy.

12. Evaluation and review

The performance of this Policy will be reported on annually and it will be formally reviewed every five years by the appropriate Corporation committee.

In addition, the effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.

Appendix A: How to share data with a third party



In order to demonstrate compliance with a third party's obligations as a Processor, an Information Security Checklist may need to be completed. The requirement for this is contained in the College's Information Security Policy.