Data Protection Policy

Responsibility of:	Data Protection Officer
Date of Approval:	10th October 2018
Review Cycle:	Every 3 years

1. Introduction

1.1. This policy sets out how the New Collaborative Learning Trust ("NCLT" or the "Trust") processes personal data.

1.2. The trust is registered with the Information Commissioner's Office (ICO)

1.3. Any questions or concerns about the operation of this policy, or if you consider that the policy has not been followed in respect of personal data about yourself or others, you should raise the matter with the Data Protection Officer (DPO) in the first instance.

1.4. All staff and students should ensure they acquaint themselves with and abide by the principles set out in this policy.

2. Definitions

2.1. **Data subjects** - includes all living individuals about whom the Trust holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

2.2. **Personal data** – refers to any information relating to a living, identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

2.3. **Data controllers** - A controller determines the purposes and means of processing personal data. In most cases the Trust would identify itself as the data controller.

2.4. **Data processors** - includes any person or organisation who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers who handle personal data on our behalf.

2.5. **Processing** - is any activity that involves the use of personal data. It includes obtaining, recording or holding data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

2.6. **Special Category Data** - includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and/or sexual orientation, genetics, and biometric information (where it is used for ID purposes). Special category data is personal data which is more sensitive, and so requires more protection.

2.7. **Third party** - means a natural or legal person, public authority, agency or body other than the data subject or controller,

3. Data Protection Principals

3.1. Data Protection legislation, consisting of the GDPR and the Data Protection Act 2018, are underpinned by six important principles. These say that personal data must:

- Be processed fairly and lawfully.
- Be processed for limited purposes and in an appropriate way.
- Be adequate, relevant and not excessive for the purpose.
- Be accurate and kept up to date.
- Not be kept longer than necessary for the purpose.
- Be secure.

3.2. Article 5(2) of the GDPR states that the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

4. Lawful basis for processing

4.1. The Trust identifies the legal basis for processing all personal data, which is recorded on the Information Asset Register.

4.2. For special category data and data relating to criminal convictions the Trust identifies additional legal basis for processing, which is also recorded on the Information Asset Register.

5. Right to be informed

5.1. Privacy Notices are issued to student applicants, enrolled students, parents/guardians of students, job applicants, and current employees in the Trust. Privacy Notices are also available on the Trust website.

5.2. Privacy notices are written in clear, plain language which is concise, transparent, easily accessible and supplied free of charge.

5.3. Privacy Notices include information about:

- The data controller
- Personal data that is collected and processed
- The purpose of collecting personal data
- The retention period
- Any third parties in receipt of personal data
- Any automated decision making and profiling
- The existence of the data subject's rights, including the right to withdraw consent and to lodge a complaint with a supervisory authority

6. Right of access

6.1. Individuals have the right to access their personal data, commonly referred to as a Subject Access Request. An individual can make a request in any format, whether verbally or written.

6.2. The identity of the subject will be verified before any information is supplied

6.3. A copy of the information will be supplied to the individual free of charge without delay and within one month of receipt of the request.

6.4. If a request is likely to take longer than one month, either because to the size or complexity of the task, of if the request falls just before the end of a term, the Trust may request up to a two month extension. Any such request will be made within one month of the receipt of the request.

6.5. The Trust may charge a reasonable fee for the administrative costs of complying with the request if the request is deemed manifestly unfounded or excessive, or if the individual requests further additional copies of their information.

6.6. If a subject access request is made electronically, the information will be provided using ShareFile. The individual will be asked to confirm their email address prior to the information being sent, and then emailed a link via an encrypted email.

7. Right to rectification

7.1. Individuals have the right to request that inaccurate personal data is rectified, or completed if it is incomplete.

7.2. Requests can be made verbally or in writing.

7.3. Requests for rectification will be responded to within one month of the request. This may be extended by a further two months if the request is deemed complex.

7.4. Any third parties holding personal data will be informed to rectify the data they hold, in line with the individual's request.

7.5. Where the Trust decides not to action the request for rectification, the Trust will explain the reason to the individual, and will inform them of their right to complain to the ICO.

8. Right to erasure

8.1. Individuals have the right to have their personal data erased. This is also known as the "right to be forgotten".

8.2. This right is not absolute, and only applies when;

- the personal data is no longer necessary for the purpose which it was originally collected or processed
- consent was identified as the lawful basis for holding the data, and the individual withdraws their consent
- legitimate interests were identified as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing
- the personal data is processed for direct marketing purposes and the individual objects to that processing; or
- there is a legal obligation

8.3. Requests for personal data erasure will be acted upon within one month of receipt of the request. This may be extended for a further two months if the request is deemed as complex.

8.4. Requests can be made verbally or in writing.

8.5. All third parties holding data on the individual will be notified to act upon the individual's request.

8.6. Providing no exceptions apply, the Trust will ensure all data held on both back up and live systems will be erased as per the individual's request.

9. Right to restrict processing

9.1. Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.

9.2. In the event of a request to restrict processing the Trust is permitted to continue to hold the data, but not to process it any further.

9.3. Individuals can request restricted processing of their data if;

- the individual contests the accuracy of their personal data and it is necessary to verify the accuracy of the data
- it is felt that the data has been unlawfully processed and the individual opposes erasure and requests restriction instead
- the personal data is no longer needed but the individual needs the Trust to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to processing their data under Article 21(1) of the GDPR, and you are considering whether your legitimate grounds override those of the individual.

9.4. Requests for restricted processing will be acted upon within one month of receipt of the request. This may be extended for a further two months if the request is deemed as complex.

9.5. Requests can be made verbally or in writing.

9.6. All third parties holding data on the individual will be notified to act upon the individual's request.

9.7. Restricted processing should be seen as a temporary measure. The Trust will notify the individual **before** the restriction is lifted.

10. Right to data portability

10.1. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

10.2. Personal data will be provided in a structured, commonly used and machine-readable form.

10.3. Personal data will only be provided once the requesting individual's identity has been verified.

10.4. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

10.5. The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

10.6. If the requested information includes information about others (i.e. third parties) the Trust would need to consider whether transmitting the data would adversely affect the rights and freedoms of those third parties.

10.7. If the requested data has been provided by multiple data subjects (e.g. a next of kin information) the Trust would need to be satisfied that all parties agree to the portability request. The Trust may have to seek agreement from all the parties involved.

10.8. Requests for personal data portability will be acted upon within one month of receipt of the request. This may be extended for a further two months if the request is deemed as complex.

10.9. Requests can be made verbally or in writing.

11. Right to object

11.1. The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. This effectively allows individuals to ask the Trust to stop processing their personal data.

11.2. Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

11.3. Individuals can also object if the processing is for:

- a task carried out in the public interest
- the exercise of official authority vested in the Trust; or
- identified legitimate interests (or those of a third party)

11.4. Individuals will be notified of their right to object at the first point of communication. In the majority of cases this will be through the Privacy Notice.

11.5. Where processing of personal data has been identified for the performance of a legal task, legitimate interests, or for research purposes, the Trust will stop processing personal data unless:

- The Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

11.6. Any decision to refuse an objection to data processing request will be considered on a case-by-case basis and will carefully consider the individual's circumstances.

11.7. If a request is refused the individual will be notified of the rationale behind the decision, and they will be reminded of their rights to make a complaint to the supervising authority.

11.8. Where processing of personal data has been identified for direct marketing purposes the Trust will stop processing as soon as the request is received.

11.9. The Trust cannot refuse a request to stop processing if an individual's objection relates to processing for direct marketing purposes.

11.10. Providing there are no exemptions, objections will be acted upon within one month of receipt of the request. This may be extended for a further two months if the request is deemed as complex.

11.11. Requests can be made verbally or in writing.

12. Rights in relation to automated decision making and profiling

12.1. Automated individual decision-making is defined as a decision made by automated means without any human involvement. Profiling is defined as automated processing of personal data to evaluate certain things about an individual.

12.2. The Trust only uses automated decision making and profiling for the performance of a contract (for staff and students).

12.3. The Trust will ensure no automated decision making or profiling is without;

- an opportunity for human intervention
- an opportunity for the individual to express their view
- an opportunity for the individual to obtain an explanation of the decision and an opportunity to challenge it.

12.4. In addition the Trust will:

- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual. This is clearly outlined in the Applicant Privacy Notice.
- use appropriate mathematical or statistical procedures
- put appropriate technical and organisational measures in place, so that you can correct inaccuracies and minimise the risk of errors
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects.

12.5. Automated decision making and profiling must not be used for processing sensitive data, unless the Trust has the explicit consent of the individual, or the processs is necessary for reasons of substantial public interests.

13. Marketing and consent

13.1. Where the trust carries out any marketing, Data Protection Laws and the Privacy and Electronic Communications Regulations (PECR) require that this is only done in a legally compliant manner. Marketing consists of any advertising or marketing communication that is directed to particular individuals.

13.2. When marketing to individuals outside of the Trust, consent will be sought at the point of data collection and thereafter on each point of contact.

13.3. Electronic marketing consent is sought on a positive, opt-in basis.

13.4. See the Marketing Policy for more information.

14. CCTV, Photographs and Images

14.1. CCTV operates on site for the purpose of site security and for the safety of individuals and the security of property on the premises, as set out in the Data Protection Impact Assessment. CCTV will be used for no other purpose.

14.2. Access to CCTV image recording will be secure and restricted to a small number of authorised staff. Images will be held for no longer than 28 days.

14.3. Clear signage will be made available to notify anyone present on site that CCTV is in operation, the purpose of CCTV, and contact details.

14.4. Consent will be sought for photographs and images in one of the following three ways;

- **Photographs or images clearly showing individuals** – consent sought at the time of capture. Subjects have the right to request deletion at any time.
- **Photographs or images of classes or small groups** – consent sought on a group basis, anyone unwilling to have their photograph or image captured should be provided with an opportunity to not be included.
- **Photographs or images of large groups of people** – usually used for events, clear notice must be given about the times and areas included in photography or image capture to allow anyone unwilling to have their photograph or image captured should be provided with an opportunity to not be included

14.5. More information about CCTV, photographs and images can be found in the CCTV, Photographs and Images Policy

15. Accountability and governance

15.1. The Trust maintains an Information Asset Register of all the data it holds. This register is reviewed and updated annually. Through the Information Asset Register the Trust identifies;

- the purpose for processing
- the identified legal basis for processing
- Descriptions of the categories of individuals and personal data
- retention periods
- Description of organisational and technical security measures
- Third party recipients of personal data

15.2. The Trust provides comprehensive, clear and transparent Privacy Notices for the data it holds about students, staff, and parents/guardians of students.

15.3. The Audit Committee oversees the governance of the Trust's approach to data protection.

16. Contracts and agreements

16.1. An individual or organisation who has access to personal data to perform a service may be classed as a processor.

16.2. The Trust will only use processors who meet the requirements of data protection legislation. Due diligence checks are used to ensure sufficient safeguards are in place to safeguard personal data.

16.3. Whenever the Trust appoints a contractor to process personal data the Trust will ensure a Data Processing Agreement is in place, outlining the data processing expectations of the Trust. For new contractors this Agreement will form part of the New Supplier Form.

17. Privacy by design & Data Protection Impact Assessments (DPIA)

17.1. The Trust adopts a "Privacy by Design" approach, and implements technical and operation measures to ensure data privacy is a high consideration in all processing activities.

17.2. The DPIA process will be used to identify and minimise the data protection risks of a project.

17.3. A DPIA will be completed whenever the use of personal data changes or if new data is being acquired, particularly if it is likely to result in a high risk to the rights and freedoms of individuals.

17.4. The Project Lead is responsible for ensuring DPIAs are completed for all new projects where the use of personal data changes or acquisition of new personal data is likely to occur.

17.5. All DPIAs must be reviewed and approved by the Data Protection Officer.

18. Data Protection Officer

18.1. The Trust has appointed a DPO whose responsibilities include:

- monitoring internal compliance
- informing and advising on data protection obligations
- providing advice regarding Data Protection Impact Assessments (DPIAs)
- supporting the Trust in demonstrating compliance
- acting as a contact point for data subjects and the supervisory authority.

18.2. The DPO will be able to operate independently and will not be dismissed or penalised for performing their tasks.

18.3. The DPO will have a high level of knowledge in data protection, and will undertake any CPD as necessary.

18.4. The DPO will be adequately resourced in order to perform their tasks.

18.5. The DPO will report to the Trust Director for Funding and Finance, and will be expected to report to Directors and Trustees relating to data protection matters.

19. Security

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

19.2. Trust staff must ensure that personal data in their working environment is secure and not in view on desks or walls.

19.3. Staff must adhere to a “clean desk” policy. Desks should be tidy with no personal data or confidential information showing.

19.4. Staff must ensure personal data, and especially sensitive information, is stored in locked drawers, filing cabinets or safes, and in lockable offices/staff areas.

19.5. Screens must be located and positioned to safeguard on-screen information.

19.6. Confidential waste bins are provided for staff at each college. Staff must ensure all paper waste containing personal data is disposed of in these bins, or shredded, rather than being placed in ordinary paper recycling or standard waste bins.

19.7. Staff must use caution when printing information that contains personal data. Staff who deal regularly with highly sensitive information must not use printers in communal areas.

19.8. Staff must not take printed or digital information off-site, except for the purposes of external meetings. The VDI Environment provides staff with a way of working off site without downloading personal data from college systems.

19.9. Removable media, such as USB drives and portable hard drives, must not be used to hold personal information unless they are password protected and fully encrypted.

19.10. Staff must only use Trust approved cloud storage systems to store or transfer data.

19.11. File uploads to the web, or any other open or public access domain must be checked first, or double checked, by a member of the senior team.

19.12. Emails containing sensitive or confidential information must be protected. Staff, Directors and Trustees must only communicate via Trust email addresses, and not use their own personal email addresses.

19.13. Where appropriate circular emails should be sent using a blind carbon copy (bcc) to ensure personal email addresses are not disclosed to other recipients.

19.14. The IT acceptable use policy must be followed to ensure robust security.

19.15. If staff use personal devices to access systems containing personal data the device must be pin or password protected.

19.16. Trust staff must not release or disclose any personal data outside the Trust to any unauthorised individuals or organisations, or inside the Trust to any staff not authorised to access the personal data without authorisation from their line manager.

20. Staff training

20.1. All staff are provided with regular and annual training and updates in data protection, outlining their rights and their responsibilities, the systems

and processes involved with data protection, and guidance in safeguarding personal data.

20.2. All new staff appointed undertake data protection training as part of the induction process.

21. Personal data breaches

21.1. A personal data breach is defined broadly and effectively as a failure to safeguard personal data, which could mean (but is not limited to);

- Losing or misplacing personal data
- Sending personal data to an incorrect recipient
- Personal data accessed or stolen without permission
- Deletion or alteration of personal data

21.2. All staff receive training on what constitutes a data breach. Posters in staff areas remind staff of what a data breach is and what to do in the event of a breach, including contact details for the DPO.

21.3. Staff should contact the DPO immediately on becoming aware of a possible personal data breach. This is to allow a quick response, further investigation and assessment, and to allow any remedial action to be put in place if required.

21.4. All breaches are recorded on the internal Personal Data Breach Register, and a Data Breach Form is completed if a further investigation is likely to take place.

21.5. If a breach is considered likely to result in a high risk to the rights and freedoms of individuals the DPO will notify both the Senior Team and the Information Commissioner's Office (ICO). Notification to the ICO will occur within 72 hours of the Trust becoming aware of the breach.

21.6. Where individuals' rights and freedoms have been compromised the Trust may notify the data subject of the breach. Action will be taken on a case-by-case basis.

21.7. More information about personal data breaches will be provided in the Trust's Personal Data Breach Policy.

22. Policy breach

22.1. Non-compliance with this policy could potentially put at risk the rights and freedoms of the data subject, lead to distress or harm, could seriously damage the reputation of the Trust, could lead to financial loss or penalties, and possible legal action. Any breach of this policy will be taken seriously and may result in disciplinary action, up to and including dismissal in serious cases.

22.2. An individual can commit a criminal offence under the Data Protection Act 2018 if they knowingly obtain and disclose personal data for their own purposes without the consent of the data controller.

23. Complaints

23.1. Complaints raised in relation to data processing will follow that set out in the Trust Complaints Policy. Complaints relating to information handling may be referred to the ICO.

24. Other documents relating to this policy:

Personal Data Breach Policy
CCTV, Photographs and Images Policy
Data Retention Schedule
IT Acceptable Use Policy
Marketing Policy
Complaints Policy