Data Protection Policy

Version 5

This policy applies to all NCLT settings.

CONTENTS

This policy includes:

- Data and Records Retention Policy
- Personal Data Breach Policy
- Biometrics Policy
-

1.0 Introduction

1.1 This policy sets out how 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 As an organisation that collects and uses personal data, the Trust takes seriously its obligations to keep personal data secure and to deal with security breaches relating to personal data if and when they arise.

1.4 Individuals who have any concerns about the operation of this policy, or who believe that the policy has not been followed in respect of their own or others' personal data, should raise the matter with the Trust Data Protection Officer (DPO) in the first instance.

1.5 Trust staff will be able to access this policy in SharePoint from the commencement of their employment and may receive periodic revisions of this policy. This policy does not form part of any Trust staff's contract of employment and the Trust reserves the right to change this policy. All staff should ensure they acquaint themselves with and abide by the principles set out in this policy. All Trust staff are obliged to comply with this policy at all times.

2.0 Scope

2.1 This policy applies to all Trust staff who collect and/or use personal data relating to individuals.

2.2 It applies to all personal data stored electronically, in paper form, or otherwise.

3.0 Legal Framework

3.1 This policy has due regard to legislation, including, but not limited to the following:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016) recognising its mandatory application to maintained schools
- Education (Independent School Standards) (England) Regulations 2010
- Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- Protection of Freedoms Act 2012
- School Standards and Framework Act 1998

3.2 This policy will also have regard to the ICO's guidance and codes of practice, subject to change in line with ICO reviews or amendments.

4.0 **Definitions**

4.1 The following are definitions as defined under the relevant data protection legislation:

- **Article** – an article under UK GDPR
- **Automated biometric recognition system**: A system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.
- **Biometric Data -** Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements
- **Data Protection Laws** – The Data Protection Act 2018, UK General Data Protection Regulation and all applicable laws relating to the collection and use of personal data and privacy, including any applicable codes of practice issued by a regulator.
- **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.
- **Data Controller** - a controller determines the purposes and means of processing personal data. In most cases, the Trust would identify itself as the data controller.
- **Data Processors** - includes any person or organisation that processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it does include suppliers who handle personal data on our behalf.
- **Data Protection Impact Assessments -** a process designed to identify and minimise data protection risks associated with processing personal data, ensuring compliance with data protection laws.
- **DPM –** Data Privacy Manager
- **DPO –** Data Protection Officer, assist's the Trust to monitor internal compliance, inform and advise on data protection obligations and act as a contact point for data subjects and the Information Commissioner's Office (ICO).
- **ICO –** Information Commissioner's Office
- **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.
- **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.
- **ROPA –** Record of Processing Activity, a central database/inventory held by the Trust to manage all processing activities in line with the ICO accountability principle.
- **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 that is more sensitive, and so requires more protection.
- **Third Party** - means a natural or legal person, public authority, agency or body other than the data subject or controller.
- **Trust** - New Collaborative Learning Trust (NCLT)

- **Trust Staff** –Trust employees or contractors who have been authorised to access any of the Trust's personal data and will include employees, consultants, contractors, and temporary staff hired to work on behalf of the Trust.
- **UK GDPR** – the UK General Data Protection Regulation

5.0 Roles and Responsibilities

5.1 This policy applies to all staff employed by the Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.2 **Trust Board**

The Trust Board has overall responsibility for ensuring that our colleges and schools comply with all relevant data protection obligations.

5.3 **Data Protection Officer**

The Data Protection Officer (DPO) is responsible for:

- overseeing the implementation of this policy
- supporting the Trust in demonstrating compliance with law
- informing and advising the Trust on data protection obligations
- reporting to the Board and Sub Committees
- supporting and advising the CEO, COO, CFO, ELT, DPM, Principal/SLT representative, Ops Officers
- providing support to the Data Protection Impact Assessments (DPIA) process
- acting as the main point of contact for data subjects and the Information Commissioner's Office (ICO).
- line management of the Data Privacy Manager (DPM)

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

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

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

The DPO will report to the Chief Executive Officer for the Trust, and will be expected to report to Directors and the Trust Executive Team in relation to data protection matters.

5.4 **Data Privacy Manager**

The Data Privacy Manager (DPM) is responsible for:

- developing related policies and guidelines where applicable.
- providing support and advice to all Trust staff on the processes and procedures associated with our Data Protection responsibilities
- providing advice regarding Data Protection Impact Assessments (DPIAs)
- acting as a point of contact for data subjects and the Information Commissioner's Office (ICO)
- managing the Trust's systems and databases to ensure records related to Data Protection are maintained in line with ICO advice and approved codes of practice.

- provide immediate local responses for establishments to:- Data Breaches and to provide SAR and FoI responses; coordinate local data protection audits; administer police requests.

The DPM will have a high level of knowledge in data protection, and will undertake any CPD as necessary. Full details of the DPM's responsibilities are set out in their job description.

The Data Protection/GDPR Team will be adequately resourced in order to perform its duties.

5.5 **Principal/Headteacher**

The Principal/Headteacher of each Trust college/school acts as the representative of the data controller on a day to-day basis. The Principal/Headteacher may have delegated a senior member of staff to liaise with the Trust's DPO/DPM.

5.6 **Operations Officers (Schools)**

School Ops Officers will:-

- provide a school point of contact to support the GDPR Team
- provide immediate school responses to data breaches working with the central GDPR Team
- provide SAR and FoI responses relevant to the school
- support school data protection audits

5.7 **Project Leads**

Project leads (Trust Leaders, Trust Managers or Heads of Faculty/Department) are responsible for:

- the notification to the GDPR Team prior to introduction of new data sharing software (including on-line systems) or data sharing agreements, or proposed material changes to processing personal data
- the provision of further information in relation to these arrangements as requested by the GDPR team.
- DPIAs being completed in conjunction with the GDPR Team before a change in data processing.

5.8 **All staff**

Staff are responsible for:

- acquainting themselves with and abide by the principles set out in this policy. All Trust staff are obliged to comply with this policy at all times, including the security requirements in paragraph 24.0.
- collecting, storing and processing any personal data in accordance with this policy
- informing the Trust and/or its schools of any changes to their personal data, such as a change of address
- contacting the DPO in the following circumstances:
    - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - if they have any concerns that this policy is not being followed
    - if they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK or European Economic Area

- if there has been a data breach
- whenever they are engaging in a new activity that may affect the privacy rights of individuals
- if they are unsure about sharing personal data with Third Parties

6.0 **Data Protection Principals**

6.1 Data Protection legislation, consisting of the UK GDPR and the Data Protection Act 2018, are underpinned by six important principles. These require personal data to be:

- processed fairly and lawfully.
- processed for limited purposes and in an appropriate way.
- adequate, relevant and not excessive for the purpose.
- accurate and kept up to date.
- kept no longer than necessary for the purpose.
- secure.

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

7.0 **Lawful Basis for Processing**

7.1 The Trust identifies the legal basis for processing all personal data, which is recorded in the Trust's Record of Processing Activity (ROPA).

7.2 Personal data will be processed under the following lawful conditions (Article 6):

- **6(1)a The data subject has given consent** to the processing of their personal data for one or more specific purposes. For children under the age of 13 consent is required from whoever holds parental responsibility for the child - unless as permitted under a preventive or counselling service.
- **6(1)b Processing is necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- **6(1)c Processing is necessary for compliance with a legal obligation** to which the controller is subject;
- **6(1)d Processing is necessary in order to protect the vital interests of the data subject** or of another natural person;
- **6(1)e Processing is necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller;
- **6(1)f Processing is necessary for the purposes of the legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

7.3 Where the lawful basis is identified as for the purposes of a legitimate interests, the Trust will conduct a Legitimate Interests Assessment (LIA).

7.4 The Trust will maintain an LIA Register, and review on a regular basis.

7.5 In addition to the standard legal basis for processing of data, special category data will also be processed under the following conditions under the UK GDPR:

- 9(2)(a) Explicit Consent
- 9(2)(b) Legal Obligations
- 9(2)(c) Vital Interests of the Data Subject
- 9(2)(d) Legitimate Basis for Processing
- 9(2)(e) Data Made Public by the Data Subject
- 9(2)(f) Legal/Judicial Capacity
- 9(2)(g) Public Interest
- 9(2)(h) Occupational Basis
- 9(2)(i) Public Health
- 9(2)(j) Archiving Purposes in the Public Interest

7.6 For special category data (Art. 9) and data relating to criminal convictions (Art. 10), conditions must also be met under sections 10 and Schedule 1 of the Data Protection Act 2018. The Trust records these additional legal bases for processing in its ROPA.

8.0 **Consent**

8.1 In most cases the data processed by the Trust will relate to other legal basis for processing, rather than consent. This is recorded in the ROPA, and is made available through the Privacy Notices.

8.2 Where consent is used, it must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

8.3 Consent will only be accepted if it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

8.4 Where consent is given, a record will be kept documenting how and when consent was given.

8.5 The Trust ensures that consent mechanisms meet the standards of all relevant data protection legislation.

8.6 Consent can be withdrawn at any time.

8.7 Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR and the Data Protection Act 2018.

8.8 Where a student is under the age of 16, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative, safeguarding, or counselling services offered directly to a student.

8.9 When gaining student consent, consideration will be given to the age, maturity and mental capacity of the student in question. Consent will only be gained from students where it is deemed that the student has a sound understanding of what they are consenting to.

9.0 **Right to be Informed**

9.1 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.

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

9.3 Privacy Notices include information such as:

- the contact details of the data controller (the Trust), including the contact details for the DPO.
- what personal data that is collected and processed.
- the legal basis for processing 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.

10.0 **Right of Access**

10.1 Individuals have the right to obtain confirmation that their data is being processed.

10.2 Under Article 15 of the UK GDPR, individuals have the right to access their personal data, commonly referred to as a Subject Access Request (SAR). An individual can make a request in any format, whether verbally or written. The Trust recognises once students reach Year 8 it usually considers that they can make decisions about their own personal data. This means that in most cases students can request access to their personal data themselves. In these circumstances the Trust does not need to ask their parents/carer to make the request.

10.3 Under the Education (Independent School Standards) (England) Regulations 2010, parents/carers of pupils in NCLT schools (defined as 'Independent schools' under section 463 of the Education Act 1996), therefore not including NCLT's sixth form colleges, have the right to receive an annual written report of the pupil's progress and attainment in the main subject areas taught.

10.4 The identity of the data subject will be verified before any information is supplied. Responses to parent/carer requests will only be made to the named contact for the student/pupil.

10.5 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.

10.6 In the event that a large quantity of information is held about an individual, the Trust will ask the requestor if more specific information can be released.

10.7 If a subject access request is likely to take longer than one month, because to the size or complexity of the task, the Trust may extend the period of compliance by a further two months. The individual will be informed of the extension, and will receive an

explanation of why the extension is necessary, within one month of the receipt of the request.

10.8 The Trust may charge a reasonable fee for the administrative costs of complying with the subject access request, if the request is deemed manifestly unfounded or excessive, or if the individual requests further additional copies of their information. All fees will be based on the administrative cost of providing the information.

10.9 Where a subject access request is manifestly unfounded or excessive, the Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to judicial remedy, within one month of the refusal.

10.10 If a subject access request is made electronically, the information will be provided in a commonly used electronic format. 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.

11.0 **Right to Rectification**

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

11.2 Requests can be made verbally or in writing.

11.3 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.

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

11.5 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 and to a judicial remedy.

12.0 **Right to Erasure**

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

12.2 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 was unlawfully processed

- the personal data is processed for direct marketing purposes and the individual objects to that processing; or
- the personal data is required to be erased in order to comply with a legal obligation.

12.3 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.

12.4 Requests can be made verbally or in writing.

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

12.6 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.

12.7 The Trust reserves the right to refuse a request for erasure where the personal data is being processed under any other legal basis except for consent.

12.8 Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies.

13.0 **Right to Restrict Processing**

13.1 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.

13.2 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.

13.3 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 NCLT processing their data under Article 21(1) of the UK GDPR, and the Trust is considering whether its legitimate grounds override those of the individual.

13.4 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.

13.5 Requests can be made verbally or in writing.

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

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

14.0 **Right to Data Portability**

14.1 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.

14.2 The right to data portability only applies in the following cases:

- to personal data that an individual has provided to a controller
- where the processing is based on the individual's consent or for the performance of a contract
- when processing is carried out by automated means.

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

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

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

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

14.7 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.

14.8 If the requested data has been provided by multiple data subjects (eg, 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.

14.9 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, ensuring the individual is informed of the reasoning behind an extension within one month of the receipt of the request.

14.10 The Trust will provide the information free of charge.

14.11 Requests can be made verbally or in writing.

14.12 Where no action is taken in response to a request, the Trust will, without delay and at least within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to judicial remedy.

15.0 **Right to Object**

15.1 The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.

15.2 Individuals have the absolute right to object to the processing of their personal data for the following purposes:

- processing is based on legitimate interests or the performance of a task in the public interest.
- processing if for direct marketing.
- processing if for purposes of scientific or historical research and statistics.

15.3 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.

15.4 Where personal data is processed for direct marketing purposes:

- the Trust will stop processing personal data for direct marketing purposes as soon as the objection is received.
- the Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

15.5 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.

15.6 Where personal data is processed for research purposes:

- the individual must have grounds relating to their particular situation in order to exercise their right to object.
- where processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

15.7 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.

15.8 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.

15.9 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.

15.10 Requests can be made verbally or in writing.

15.11 Where the processing activity is outlined above, but is carried out online, the Trust will offer a method for individuals to object online.

16.0 Rights in Relation to Automated Decision Making and Profiling

16.1 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.

16.2 Individuals have the right not to be subject to a decision when:

- it is based on automated processing.

16.3 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.

16.4 In addition the Trust will:

- ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- use appropriate mathematical or statistical procedures.
- implement appropriate technical and organisational measures, so that individuals 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.

16.5 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 process is necessary for reasons of substantial public interests.

17.0 Marketing and Consent

17.1 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.

17.2 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.

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

17.4 A register of consent, when it was given and for what project, will be kept and reviewed on a regular basis.

18.0 **CCTV**

18.1 A separate policy has been approved by the Trust in relation to the operation of CCTV.

18.2 The Trust understands that recording images of identifiable individuals constitutes as processing personal information, as defined by data protection legislation, and processing of images is done so in line with data protection principles.

18.3 The Trust operates CCTV at its establishments for the reasons set out in the CCTV Policy, including: site security; the safety of individuals and the security of property on the premises. CCTV will be used for no other purpose than identified in the CCTV Policy.

18.4 Access to CCTV image recording equipment is secure and restricted to a small number of authorised staff.

18.5 Any downloaded images will be held for no longer than is necessary and authorised users will only retain them for a maximum of 28 days, following any request for use/access, unless further retention is permitted under Data Protection laws, such as legal proceedings.

18.6 Clear signage will be made available to notify anyone present on site that CCTV is in operation..

18.7 Where the Trust needs to obtain consent for processing of photographs or images it will be sought in one of the following three ways:

- **Photographs or images clearly showing individuals** – consent sought/confirmed 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

18.8 In addition to the above, for students under the age of 16 written permission will be sought from parents or carers if the Trust wishes to use images/videos of students in any publications or marketing capacity.

18.9 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from UK GDPR and the Data Protection Act 2018.

19.0 **Protection of Biometric Information**

19.1 Where the Trust collects and processes children's biometric data it will be in accordance with data protection laws and section 26 of the Protection of Freedoms Act 2012.

19.2 Where the Trust looks to process a child's biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive school meals instead of paying with cash) it will comply with the Protection of Freedoms Act 2012 which requires consent before processing biometric data.

19.3 Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA must be carried out.

19.4 Reasonable steps will be made to ensure each parent or carer of a pupil or student is approached to seek written consent. This will be undertaken through the Admission Form. The Trust will not need to approach a particular parent/carer to seek consent where:-

- the parent/carer cannot be found, for example, their whereabouts or identity is not known.
- the parent/carer lacks the mental capacity to object or to consent.
- the welfare of the child requires that a particular parent/carer is not contacted, for example where a child has been separated from an abusive parent/carer who is not to be informed of the child's whereabouts.
- where it is otherwise not reasonably practicable for a particular parent/carer to be notified or for their consent to be obtained.

19.5 Where a child is being 'looked after' by the Local Authority (LA) or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified and their written consent requested.

19.6 Correspondence to parents/carers/the relevant organisation will include details on:-

- the type of biometric information to be taken.
- how the data will be used/processed.
- the parent's/carer's and the pupil's right to refuse or withdraw their consent.
- the Trust's duty to provide reasonable alternative arrangements for any child whose information cannot be processed (such as the issuance of a unique PIN number or an alternative which will not represent a disadvantage or additional burden).

and state the Trust will not process the biometric data of a child under the age of 18 in the following circumstances:-

- the child (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data.
- no parent or carer has consented in writing to the processing.
- a parent/carer has objected in writing to such processing, even if the other parent/carer has given written consent.

and include the explanation that a child and/or their parents/carers can object to participation in the Trust's biometric system(s) or withdraw their consent at any time.

19.7 The Trust will not process the biometric data of a child under the age of 18 in the following circumstances:

- the child (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data.
- no parent or carer has consented in writing to the processing.
- a parent/carer has objected in writing to such processing, even if the other parent/carer has given written consent.

19.8 Where consent is withdrawn by a child and/or their parents/carers, the biometric data will be deleted.

19.9 Staff and other adults can object to taking part in a biometric system(s) and can withdraw their consent at any time. In such cases, all biometric data relating to the individual will be deleted.

20.0 **Data and Records Retention**

20.1 The Trust takes seriously its obligations and responsibilities to ensure data is only held for the period of time needed to meet the requirements of its collection. Data will not be kept for any longer than is necessary.

20.2 The Trust maintains the Record of Processing Activity (ROPA). ROPA includes information about how long data is held by the Trust and is updated on a regular basis, in collaboration with Project leads.

20.3 Records are retained in different formats for different processing purposes. Where records are retained in physical (paper format), the Trust places these records in secure locations, where only appropriate access is provided. Any queries or further information relating to records storage should be sent to the Trust GDPR Team via Data.Protection@nclt.ac.uk.

20.4 Retention periods for different types of data are outlined in the retention schedule in the ROPA. Trust Project leads have access to this and are fully aware of the retention periods involved in the data processed within their department.

20.5 NCLT utilise a Data Domain and Veeam backup and recovery platform, Data Domain systems are the only solution built with relentless attention to data integrity, giving NCLT ultimate confidence in recoverability. The innovative Data Invulnerability Architecture lays out the industry's best defence against data integrity issues. Data Domain natively provides device-based encryption, data consistency and integrity checks; verifying that the data being backed up matches the live data and has not been amended or edited in any way.

20.6 The Trust has in place a contract with reputable confidential waste disposal companies, whereby regular or on demand collections and visits are made at each Trust site and the waste collected in the secure waste bins is shredded into a waste vehicle on site. Destruction certificates are then made available to the Trust via a web-based portal, which provides information related to each visit.

20.7 The Trust also holds a contract with a company who support us to dispose of IT equipment and electronic devices to ensure compliance with the ICO's accountability principle. Certificates of destruction are provided to the Trust Director of IT.

20.8 Unrequired data will be deleted as soon as is practicable.

21.0 **Accountability and Governance**

21.1 The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the relevant data protection legislation.

21.2 The Trust maintains a ROPA of all the data it holds.

21.3 The Trust maintains records of activities relating to higher risk processing, such as the processing of special category data or that in relation to criminal convictions and offences.

21.4 The Trust provides comprehensive, clear and transparent Privacy Notices.

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

22.0 **Data Sharing Agreements**

22.1 Any form of data sharing will be done so following the data protection legislation, as set out in the UK GDPR and Data Protection 2018.

22.2 Before sharing data a DPIA will be conducted, where necessary, to establish the risks involved with sharing, and highlight any safeguards that need to be put in place.

22.3 The DPIA will establish whether a Data Sharing Agreement will need to be put in place. This includes all forms of data sharing, including:

- routine data sharing
- ad hoc or one-off sharing
- data pooling.

22.4 A register of all Data Sharing Agreements will be kept and reviewed on a regular basis.

23.0 **"Privacy by Design" and Data Protection Impact Assessments (DPIA)**

23.1 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. Such measures include:

- data minimisation
- pseudonymisation
- transparency

- allowing individuals to monitor processing
- continuously creating and improving security features.

23.2 Data Privacy Impact Assessments will be used to identify the most effective method of complying with the Trust's data protection obligations.

23.3 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.

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

23.5 The Trust will ensure that all DPIAs include the following information:

- a description of the processing operations and purposes.
- who will be affected.
- an assessment of the necessity and proportionality of the processing in relation to the purpose.
- an outline of the risks to individuals .
- the measures implemented in order to address risk.
- how the processing activity will be communicated to data subjects.

23.6 Where a DPIA indicates a high 'residual risk' after all mitigating measures have been identified it is unlikely the Trust would proceed. A DPIA with a high residual risk would require the Trust to consult the ICO to seek it's opinion as to whether the proposed processing operation would comply with data protection obligations.

23.7 All DPIAs will be recorded on a DPIA Register, and reviewed on a prioritised basis.

24.0 **Security**

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

24.2 Before sharing data, all staff members will ensure that:

- they are allowed to share it.
- that adequate security is in place to protect it.
- our obligations under data protection legislation are being met

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

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

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

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

24.7 Visitors or contractors who have access to areas containing sensitive information, either electronically or physically, should be supervised at all times.

24.8 Confidential waste bins are provided for staff at each college/school. 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.

24.9 Staff must use caution when printing information that contains personal data. Staff who deal regularly with highly sensitive information should avoid using printers in communal areas.

24.10 Staff should avoid taking printed or digital information off-site, except for the purposes of external meetings, trips and visits, etc. The VDI Environment provides staff with a way of working off site without downloading personal data from college or school systems.

24.11 Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to safeguard personal information. The person taking the information off-site accepts full responsibility for the security of the data.

24.12 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

24.13 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.

24.14 All electronic devices are pin or password-protected to protect the information on the device.

24.15 Staff should refrain from saving passwords and should regularly clear their cache, especially when working on devices with multiple users.

24.16 Where possible the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

24.17 Where data is saved on removable storage or a portable device, the device should be kept in a locked filing cabinet, drawer or safe when not in use.

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

24.19 Members of staff are provided with their own secure login and password, which must be kept safe and secure at all times.

24.20 Emails containing sensitive or confidential information must be password-protected, and encrypted.

24.21 Staff must only communicate via Trust email addresses, and not use their own personal email addresses. Directors, Advisors and Trustees will be contacted via their personal email addresses to remind them of upcoming meetings. They will access

meeting documents via a secure SharePoint site logging in using their NCLT email address and password.

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

24.23 The IT Acceptable Use Policy must be followed to ensure robust security.

24.24 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.

24.25 The physical security on site is the responsibility of the Estates Manager for the Trust. The security of the site should be reviewed on a regular basis, and furniture or furnishing requests to secure physical storage of personal data should be made to the Estates Manager.

24.26 The Trust Director of IT is responsible for ensuring all security measures are in place to safeguard the network from external threats, and to make regular secure backups from the server. The Trust Director of IT also oversees the breach detection software, and will alert the DPO/DPM and Senior staff in the event of any significant potential threats.

25.0 **Staff Training**

25.1 All staff are provided with regular 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.

25.2 Refresher training for all staff takes place every two years during the academic year in which it is due.

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

26.0 **Publication of Information**

26.1 The Trust will not publish any personal information, including photographs, without the permission of the affected individual, or with parental consent if under the age of 16.

26.2 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.

27.0 **DBS Data**

27.1 All data provided by the DBS will be handled in line with data protection legislation, which includes electronic communication.

27.2 Data provided by the DBS will never be duplicated.

27.3 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

28.0 **Personal Data Breaches**

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

28.2 Personal data breach is defined as any failure to keep personal data secure, which leads to the accidental or unlawful loss (including loss of access), destruction, alteration or unauthorised disclosure of personal data, which could mean (but is not limited to):

- loss or theft of personal data or equipment that stores personal data;
- loss or theft of personal data or equipment that stores the Trust's personal data from a Trust supplier;
- inappropriate access controls meaning unauthorised Trust staff can access personal data;
- any other unauthorised use of or access to personal data;
- deleting personal data in error;
- human error (which could be as simple as putting a letter in the wrong envelope or leaving a phone or laptop containing personal data on a train);
- hacking attack; infection by ransom ware or any other intrusion on our systems/network;
- 'blagging' offences where information is obtained by deceiving the organisation who holds it; or
- destruction or damage to the integrity or accuracy of personal data.

28.3 A personal data breach can also include:

- equipment or system failure that causes personal data to be temporarily unavailable;
- unforeseen circumstances such as a fire, flood or power failure that causes personal data to be temporarily unavailable;
- inability to restore access to personal data, either on a temporary or permanent basis; or
- loss of a decryption key where personal data has been encrypted because this means the Trust cannot restore access to the personal data.

28.4 The Principal/Headteacher at each school or college is responsible for ensuring that all staff understand what constitutes a data breach, and how to respond to a data breach.

28.5 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 Trust GDPR Team.

28.6 Trust Staff must immediately notify any personal data breach to the DPM or DPO, no matter how big or small and whether or not Trust staff think a breach has occurred or is likely to occur. This allows the Trust to contain the breach as soon as possible and to consider a recovery plan to minimise any risk of damage to the individuals affected and to the Trust.

28.7 If Trust staff discover a personal data breach outside working hours, Trust staff must notify it to the Trust's DPO by email as soon as possible.

28.8 There are four elements to managing a personal data breach or a potential one as listed below:

- containment and recovery.
- assessment of on-going risk.
- notification.
- evaluation and response.

Each element is explained in more detail in Appendix A.

28.9 At all stages the DPM/DPO, Trust Managers and senior leaders will consider whether the breach is within scope of the NCLT Business Continuity Plan, and will consider whether to seek external legal advice.

28.10 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.

28.11 If a breach is considered likely to result in a high risk to the rights and freedoms of individuals the DPM/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.

28.12 The risk of the breach affecting the individual rights and freedoms of individuals, and the decision to notify the ICO, will be considered on a case-by-case basis.

28.13 In cases where there is deemed to be a high risk to individual rights and freedoms of an individual the Trust will notify those concerned directly.

29.0 **Policy Breach**

29.1 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, and 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.

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

30.0 **Complaints**

30.1 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.

31.0 **Other documents relating to this policy:**

CCTV Policy
IT Acceptable Use Policy
Complaints Policy
Business Continuity Plan
Disaster Recovery Policy

Appendix A

The Four Elements of Managing a Personal Data Breach

- Containment and recovery.
- Assessment of on-going risk.
- Notification.
- Evaluation and response.

Containment and Recovery
An initial assessment of the personal data breach will be carried out, using the Data Breach Severity Tool in Appendix C.

If the personal data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected then it will be added to the Trust's Data Breach Register and no further action will be taken.

If the personal data breach is likely to impact on the rights and freedoms of the individuals affected then the Trust will put together and implement a bespoke Personal Data Breach Plan to address the breach concerned in accordance with the Trust's Data Breach Notification Procedure. This will include consideration of:

- whether there are any other people within the Trust who should be informed of the breach, such as IT team members, to ensure that the breach is contained;
- what steps can be taken to contain the breach, recover the loss of any personal data or to prevent damage being caused; and
- whether it is necessary to contact other third parties such as students, parents, banks, the ICO or the police particularly in the case of stolen personal data. All notifications shall be made by the Data Protection Officer.

All actions taken in relation to a personal data breach will be in accordance with the Data Breach Notification Procedure, which is maintained and administered by the Data Protection Manager (see Appendix B).

The Data Protection Officer is responsible for ensuring that the Data Breach Register is updated.

Assessment of Ongoing Risk
As part of the Trust's response to a personal data breach, once the breach has been contained the Trust will consider the on-going risks to the Trust and to any other party caused by the breach and what remedial action can be taken to minimise the impact of the breach. This will be undertaken in accordance with the Trust's Data Breach Notification Procedure.

Notification
Under Data Protection Laws, the Trust may have to notify the ICO and also possibly the individuals affected about the personal data breach.

Any notification will be made by the Data Protection Officer following the Trust's Data Breach Notification Procedure. The notification shall comply with the requirements of the ICO.

Notification of a personal data breach must be made to the ICO without undue delay and where feasible within 72 hours of when the Trust becomes aware of the breach unless it is unlikely to result in a risk to the rights and freedoms of individuals. It is therefore imperative that Trust staff notify all personal data breaches to the Trust in accordance with the Data Breach Notification Procedure immediately.

Notification of a Personal Data breach must be made to the individuals affected without undue delay where the breach is likely to result in a high risk to the rights and freedoms of individuals.

Not all personal data breaches are notifiable to the ICO and/or the individuals affected and the Trust will decide whether to notify and who to notify in accordance with the Data Breach Notification Procedure.

Where the personal data breach relates to a temporary loss of availability of the Trust's systems, the Trust does not have to notify if the lack of availability of personal data is unlikely to result in a risk to the rights and freedoms of individuals. The Trust does not consider that it has any systems where temporary unavailability would cause a risk to the rights and freedoms of individuals but this will be assessed on a case-by-case basis in accordance with the Data Breach Notification Procedure.

In the case of complex breaches, the Trust may need to carry out in-depth investigations. In these circumstances, the Trust will notify the ICO with the information that it has within 72 hours of awareness and will notify additional information in phases. Any delay in notifying the ICO must be seen as exceptional and shall be authorised in accordance with the Data Breach Notification Procedure.

Where a personal data breach has been notified to the ICO, any changes in circumstances or any relevant additional information which is discovered in relation to the personal data breach shall also be notified to the ICO in accordance with the Data Breach Notification Procedure.

When the Trust notifies the affected individuals, it will do so in clear and plain language and in a transparent way. Any notifications to individuals affected will be in accordance with the Data Breach Notification Procedure. Any notification to an individual should include details of the action the Trust has taken in relation to containing the breach and protecting the individual. It should also give any advice about what they can do to protect themselves from adverse consequences arising from the breach.

The Trust may not be required to notify the affected individuals in certain circumstances as exemptions apply. Any decision whether to notify the individuals shall be done in accordance with the Data Breach Notification Procedure and shall be made by the Data Protection Officer.

Evaluation and Response

It is important not only to investigate the causes of the breach but to document the breach and evaluate the effectiveness of the Trust's response to it and the remedial action taken.

There will be an evaluation after any breach of the causes of the breach and the effectiveness of the Trust's response to it. All such investigations shall be carried out in accordance with the Data Breach Notification Procedure and will be recorded on the Personal Data Breach Register.

Any remedial action such as changes to the Trust's systems, policies or procedures will be implemented in accordance with the Data Breach Notification Procedure.

Appendix B

Data Protection Notification Procedure

IDENTIFYING AND REPORTING A DATA BREACH

If you discover a data breach, however big or small, you must report this to our Data Protection Officer immediately.

The Data Protection Officer can be contacted at: 01977 702139, data.protection@nclt.ac.uk.

Any other questions about the operation of this procedure or any concerns that the procedure has not been followed should be referred in the first instance to the Data Protection Officer.

A data breach could be as simple as you putting a letter in the wrong envelope and therefore even the most minor data breaches ***must*** be reported.

False alarms or even breaches that do not cause any harm to individuals or to the Trust should nevertheless be reported as it will enable us to learn lessons in how we respond and the remedial action we put in place.

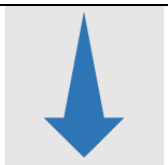
We have a legal obligation to keep a register of all data breaches, no matter how big or small and no matter whether any harm was caused.

BECOMING AWARE OF A DATA BREACH – INVESTIGATING

We become aware of a data breach when we have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. From this point, our time limit for notification to the ICO will commence.

When you report a data breach to our Data Protection Officer, our Data Protection Officer will promptly investigate the breach to ascertain whether we are fully aware that a breach has occurred that has led to personal data being compromised.

THIS WILL BE DONE WITHIN 24 HOURS OF A BREACH BEING REPORTED TO US.



ASSESSING A DATA BREACH

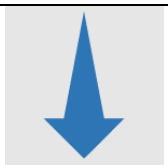
Once you have reported a breach and our Data Protection Officer has investigated it and has decided that we are aware that a breach has occurred, our Data Protection Officer will log the breach in our Data Breach Register and will carry out an initial assessment of the breach to evaluate its severity.

Once the level of severity is known, our Data Protection Officer will notify management. Where necessary, the Trust may need to follow the **Trust's Disaster Recovery Plan**.

We will then investigate the breach and consider any on-going risks to the Trust and any individuals affected.

If our Data Protection Officer and management consider that the breach is very serious, they will consider the impact on our reputation and the effect it may have on the trust placed in us. Our Data Protection Officer and senior management will consider whether to appoint a PR professional to advise on reputational damage and will also consider whether legal advice is needed.

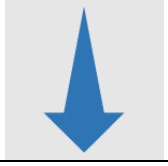
THIS WILL BE DONE WITHIN 24 HOURS OF US BECOMING AWARE OF THE BREACH.



FORMULATING A RECOVERY PLAN

Our Data Protection Officer and senior management will investigate the breach and consider a recovery plan to minimise the risk to individuals. As part of the recovery plan, our Data Protection Officer and senior management may interview any key individuals involved in the breach to determine how the breach occurred and what actions have been taken.

THIS WILL BE DONE WITHIN 24 HOURS OF ASSESSING THE BREACH.



NOTIFYING A DATA BREACH TO THE ICO

Appendix C sets out the methodology in determining whether a breach is reportable to the ICO.

Where required, the notification to the ICO must be within 72 hours of becoming aware of the breach.

The content of the notification will be drafted by our Data Protection Officer in line with our Data Breach Policy, and the notification will be made by our Data Protection Officer – please be aware that **under no circumstances must you try and deal with a data breach yourself**.

THIS WILL BE DONE WITHIN 72 HOURS OF BECOMING AWARE OF THE BREACH.

NOTIFYING A DATA BREACH TO INDIVIDUALS

Where the incident is categorised by the methodology in Appendix C as High or Very High we must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by our Data Protection Officer in line with our Data Breach Policy and in conjunction with consulting the ICO if considered necessary. We will notify individuals in clear and plain language and in a transparent manner (for example by email, SMS or letter). **Please be aware that under no circumstances must you try and deal with a data breach yourself.**

In some circumstances, explained in our Data Breach Policy, we may not need to notify the affect individuals. Our Data Protection Officer will decide whether this is the case.

THIS WILL BE DONE AS SOON AS POSSIBLE AFTER WE BECOME AWARE OF THE BREACH.

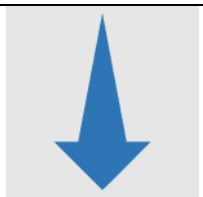
NOTIFYING A DATA BREACH TO OTHER RELEVANT THIRD PARTIES

We may also consider that it is necessary to notify other third parties about the data breach depending on the nature of the breach. This could include:

- Insurers
- Police
- Employees
- Parents/Guardians
- Sponsors
- Banks
- Contract counterparties

The decision as to whether any third parties need to be notified will be made by our Data Protection Officer and management. They will decide on the content of such notifications.

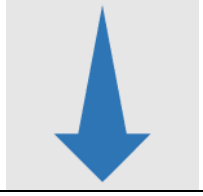
THIS WILL BE DONE WITHIN 5 DAYS OF BECOMING AWARE OF A DATA BREACH.



CONSIDER WHETHER NOTIFICATIONS NEED TO BE UPDATED

We need to keep the ICO up to date about the data breach. If anything changes from the time we send the initial notification to the ICO, our Data Protection Officer will consider whether we need to update the ICO about the data breach.

THIS WILL BE CONSIDERED ON AN ONGOING BASIS.



EVALUATION AND RESPONSE

The key to preventing further incidents is to ensure that the Trust learns from previous incidents.

It is extremely important to identify the actions that the Trust needs to take to prevent a recurrence of the incident. Our Data Protection Officer and management will carry out an evaluation as to the effectiveness of our response to the data breach and document this in our Data Breach Register.

Appendix C – Breach Categorisation

1.1 The severity of the Breach will be calculated using the ENISA assessment. Where the assessment score does not categorise the incident as High or Very High, and the data subjects(s) would avoid any significant inconveniences, the ICO self-assessment reporting tool will be used to assess the significance of the breach.

1.2 ENISA Assessment
The ENISA Breach Severity Tool is accessible at:
https://www.enisa.europa.eu/publications/dbn-severity

Severity = (Data Processing Context x Ease of Identification) + Circumstances of Breach

SE = (DPC x EI) + CB

Severity of a Data Breach		
SE < 2	**Low**	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.)
2 < SE < 3	**Medium**	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 < SE < 4	**High**	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.)
4 < SE	**Very high**	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

ICO Breach Assessment

1.3 Where the assessment score does not categorise the incident as High or Very High, and the data subjects(s) would avoid any significant inconveniences (as set out in the table above) the ICO self-assessment reporting tool will be used to assess the significance of the breach. The current ICO process includes the following mitigation assessment:-

Do you consider the data to be contained and the risk to data subjects mitigated?

To assist you assess the risk to the data subject consider if the personal data concerned is contained:

- *has any lost data been located?*
- *was the data sent to a trusted recipient?*
- *have you asked the recipient to return the data or securely dispose of it?*
- *have steps been taken to confirm the recipient has returned or securely disposed of the data?*
- *did the recipient proactively contact you to advise you of the breach?*
- *was the data encrypted or password protected or now beyond use?*

Considering the above points (which is not exhaustive), where the response is 'Yes' then the incident is not reportable to the ICO.

1.4 The Data Processing Context (DPC), Ease of Identification (EI) and Circumstance of Breach (CB) Scoring are provided below.

Data Processing Context (DPC) Scoring

Table 1: Data Processing Context (DPC)		Score
Simple data	Eg. biographical data, contact details, full name, data on education, family life, professional experience, etc.	
	Preliminary basic score: when the breach involves ''simple data'' and the controller is not aware of any aggravating factors.	**1**
	The DPC score could be increased by 1, e.g. when the volume of "simple data" and/or the characteristics of the controller are such that certain profiling of the individual can be enabled or assumptions about the individual's social/financial status can be made.	2
	The DPC score could be by 2, e.g. when the "simple data" and/or the characteristics of the controller can lead to assumptions about the individual's health status, sexual preferences, political or religious beliefs.	3
	The DPC score could be increased by 3, e.g. when due to certain characteristics of the individual (e.g. vulnerable groups, minors), the information can be critical for their personal safety or physical/psychological conditions.	4
Behavioural data	Eg. location, traffic data, data on personal preferences and habits, etc.	
	Preliminary basic score: when the breach involves ''behavioural data'' and the controller is not aware of any aggravating or lessening factors.	**2**
	The DPC score could be decreased by 1, e.g. when the nature of the data set does not provide any substantial insight to the individual's behavioural information or the data can be collected easily (independently from the breach) through publicly available sources (e.g. combination of information from web searches).	1
	The DPC score can be increased by 1, e.g. when the volume of "behavioural data" and/or the characteristics of the controller are such that a profile of the individual can be created, exposing detailed information about his/her everyday life and habits.	3
	The DPC score can be increased by 2, e.g. if a profile based on individual's sensitive data can be created.	4
Financial data	Any type of financial data (e.g. income, financial transactions, bank statements, investments, credit cards, invoices, etc.). Includes social welfare data related to financial information.	
	Preliminary basic score: when the breach involves ''financial data'' and the controller is not aware of any aggravating or lessening factors.	**3**
	The DPC score could be decreased by 2, e.g. when the nature of the data set does not provide any substantial insight to the individual's financial information (e.g. the fact that a person is the customer of a certain bank without further details).	1
	The DPC score could be decreased by 1, e.g. when the specific data set includes some financial information but still does not provide any significant insight to the individual's financial status/situation (e.g. simple bank account numbers without further details).	2
	The DPC score could be increased by 1, e.g. when due to the nature and/or volume of the specific data set, full financial (e.g. credit card) information is disclosed that could enable fraud or an detailed social/financial profile is created.	4
Sensitive data	Any type of sensitive data (e.g. health, political affiliation, sexual life)	
	Preliminary basic score: when the breach involves 'sensitive data'' and the controller is not aware of any lessening factors.	**4**
	The DPC score could be decreased by 1, e.g. when the nature of the data set does not provide any substantial insight to the individual's behavioural information or the data can be collected easily (independently from the breach) through publicly available sources (e.g. combination of information from web searches).	1
	The DPC score could be decreased by 2, e.g. when nature of data can lead to general assumptions.	2
	The DPC score could be decreased by 1, e.g. when nature of data can lead to assumptions about sensitive information.	3

Ease of Identification (EI) Scoring

(see annex 2 for examples - https://www.enisa.europa.eu/publications/dbn-severity)

Negligible = 0.25
Limited = 0.5
Significant = 0.75
Maximum = 1

Circumstance of Breach (CB) Scoring

A1 - Loss of Confidentiality	
0	Examples of data exposed to confidentiality risks without evidence that illegal processing has occurred: • a paper file or laptop is lost during transit. • equipment has been disposed without destruction of the personal data.
0.25	Examples of data disposed to a number of known recipients: • an email with personal data has been wrongly sent to a number of known recipients. • some customers could access other customers' accounts in an online service.
0.5	Examples of data disposed to an unknown number of recipients: • data are published on an internet message board. • data are uploaded to a P2P site. • an employee sells a CD ROM with customer data. • a wrongly configured website makes data from internal users publicly accessible on the Internet.
A2 - Loss of Integrity	
0	Examples of data altered but without any identified incorrect or illegal use: • the records of a database with personal data have been wrongly updated but the original has been obtained before any use of the altered data occurred.
0.25	Examples of data altered and possibly used in an incorrect or illegal way but with possibility to recover: • a record that is necessary for the provision of an online social service has been changed and the individual needs to ask for the service in an offline way. • a record that is important for the accuracy of an individual's file in an online medical service has been changed.
0.5	Examples of data altered and possibly used in an incorrect or illegal way without possibility to recover: • the previous examples + the original cannot be recovered.
A3 - Loss of Availability	
0	Examples of data being recoverable without any difficulty: • a copy of file is lost but other copies are available. • a database is corrupted but can be easily reconstructed from other databases.
0.25	Examples of temporal unavailability: • a database is corrupted but can be reconstructed from other databases, although some processing is required. • a file is lost but the information can be provided again by the individual.
0.5	Examples of full unavailability (data cannot be recovered from the controller or the individuals): • a file is lost/database corrupted, there is not back up of this information, and it cannot be provided by the individual.
A4 - Malicious Intent	

0.5	The breach was due to an intentional action, e.g., in order to cause problem to the data controller (e.g., demonstrate loss of security) and/or in order to harm the individuals. • an employee of a company intentionally shares private data from customers in a social media public site. • an employee of a company sells private data from customers to another company. • a member of a social network intentionally sends information about other members to their family members in order to harm them.

Equality Impact Assessment (EIA)

The completion of this document is a requirement for all existing and proposed New Collaborative Learning Trust (NCLT) policies, major procedures, practices and plans (hereafter referred to as policies) as well as whenever looking at policy updates.

The Equality Act 2010 sets out our legal duty to undertake equality analysis of all trust/college policies. Completion of this EIA is the first step in meeting this duty. Please send the completed EIA (together with a copy of the related policy/draft policy document) to the Chief of People Operations who will review the document and may refer to the Equality and Diversity Committee as necessary to advise on any follow up action that might be required.

Completion of the Equality Impact Assessment is part of the Specific Equality Duties (SED) required of the trust. Over arching the specific duties is the General Equality Duty (GED) required of everyone. Please bear the GED and SED in mind when undertaking this audit.

General Equality Duty

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act.
- Advance equality of opportunity between people who share a protected characteristic and those who do not.
- Foster good relations between people who share a protected characteristic and those who do not.

Specific Equality Duties Relevant to EIA are to provide:

- Sufficient information to demonstrate compliance with the general duties; including effects policies have on people.
- Evidence that analysis of this information has been undertaken.
- Details of information considered during analysis.
- Details of engagement (consultation) that has taken place.

Protected Characteristics are:

- Age
- Disability
- Gender Reassignment
- Marriage/Civil Partnership
- Pregnancy/Maternity Leave
- Race
- Religion or Belief
- Sex
- Sexual Orientation

Audit Prompt	Response
Name of policy	Data Protection Policy
Author of document:	Richard Wheatcroft
Responsible Senior Manager:	Richard Wheatcroft

Briefly describe the aims, objectives and purpose of the policy.	To ensure that personal data is secure and is processed in line with DPA, GDPR and ICO guidance.
Who does the policy apply to: • Staff • Learners (please indicate which groups) • Members of the general public (please specify)	All the three areas covered in the bullet points. This policy governs the processing of data which covers each area.
Will the policy affect members of the target audience equally? If no, please indicate the specific groups targeted by the policy. In targeting the policy at a specific group of people will members of other groups be disadvantaged? If yes, how will this be addressed? What information has been gathered about the diversity of the target audience? Attach details of information considered. How has this diversity been taken into account in writing the policy?	Yes No The target audience will be all staff, learners and member of the general public who have personal data processed. The policy is written to ensure that all processes are consistent. It also highlights special character data and the associated processes and safeguards attached to this data
Does this policy contain visual images? If yes, are these technical or cultural in nature? If cultural, do they reflect diversity? If yes, please indicate how.	Yes, flow charts which are technical and not cultural.
Please indicate how this policy supports the trust/college in its General Equality Duty to: • Eliminate unlawful discrimination, harassment and victimisation (A). • Advance equality of opportunity between people who share a protected characteristic and those who do not (B). • Foster good relations between people who share a protected characteristic and those who do not (C).	Ensure that there are clear processes that ensure consistency of operations and requests for access across the trust.
Please indicate any negative impacts identified in relation to the protected characteristics listed below, or how you have arrived at the view that there are not negative impacts in relation to these characteristics:	There should be no negative impacts on the identified characteristics as the processes involved are consistent.

Age Disability Gender Reassignment Marriage/Civil Partnership Pregnancy/Maternity Leave Race Religion or Belief Sex Sexual Orientation	
Is the policy free from discrimination on the grounds of: • Additional Learning Needs • Economic Needs • Social Needs	Yes
Please indicate who the policy has been considered by and/or who has been consulted about the policy. Where applicable include: • Staff/student consultative groups • Trade unions • Equality and Diversity, Health and Safety and Safeguarding Committee • Other committees/working groups (specify) • Senior Management Team • Trust Executive Team • Board of Directors • External group / Advisory group (specify)	The trust executive will review the policy Key trust leaders/managers have been involved in the creation of the process in previous versions. The Data Privacy manager will oversee the policy and ensure requests are consistently processed in the required times set out in the policy.
Can you identify any further consultations that might be necessary to ensure no adverse impact? If yes, please specify.	No
Can you identify any differential or adverse impact the policy might have that is not already recorded? If yes, please specify.	No

How would you assess the overall impact of this policy on equality? Please circle.	High / **Medium** / Low
Please record who this audit has been completed by (if by committee/work group please indicate and get lead person to sign off):	Name : Richard Wheatcroft Job Title : Trust Director Date : April 25

Please send the completed EIA (together with a copy of the related policy) to Ellie Lightowler (HR Officer). Where necessary the policy will be reviewed by the Equality and Diversity Committee who may require additional information to fully analyse the impact of the policy and any actions/changes needed to address any negative impacts identified.