newcollaborative
Learning Trust

Data Protection Policy

Version 2

CONTENTS PAGE

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. Legal Framework

2.1. This policy had due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

2.2 This policy will also have regard to the ICO's guidance and codes of practice

3. Definitions

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

- **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.
- **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.
- **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.

- **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.
- **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.
- **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,

4. Data Protection Principals

4.1. Data Protection legislation, consisting of the UK 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.

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

5. Lawful basis for processing

5.1. The Trust identifies the legal basis for processing all personal data, which is recorded on the Record of Processing Activity (ROPA).

5.2. Under the relevant data protection legislation, data will be processed under the following conditions:

- **6(1)a The data subject has given consent** to the processing of his or her personal data for one or more specific purposes;
- **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.

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

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

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

5.6. 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

5.7. In addition to the conditions under Article 9 of the UK GDPR, conditions must also be met under Schedule 1 of the Data Protection Act 2018.

6. Consent

6.1. 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.

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

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

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

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

6.6. Consent can be withdrawn at anytime.

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

6.8. 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.

6.9. 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.

7. Right to be informed

7.1. 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.

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

7.3. Privacy Notices include information such as:

- The contact details of the data controller (the Trust), including the contact details for the Data Protection Officer
- 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

8. Right of access

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

8.2. 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.

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

8.4. 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.

8.5. In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

8.6. 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 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.

8.7. 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. All fees will be based on the administrative cost of providing the information.

8.8. Where a 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.

8.9. If a subject access request is made electronically, the information will be provided 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.

8.10. The DPO will analyse and report on all Subject Access Requests.

9. Right to rectification

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

9.2. Requests can be made verbally or in writing.

9.3. 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.

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

9.5. 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.

10. Right to erasure

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

10.2. 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

10.3. 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.

10.4. Requests can be made verbally or in writing.

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

10.6. 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.

10.7. 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.

10.8. 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

11. Right to restrict processing

11.1. 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.

11.2. 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.

11.3. 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 UK GDPR, and you are considering whether your legitimate grounds override those of the individual.

11.4. 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.

11.5. Requests can be made verbally or in writing.

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

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

12. Right to data portability

12.1. 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.

12.2. 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

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

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

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

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

12.7. 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.

12.8. 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.

12.9. 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.

12.10. The Trust will provide the information free of charge.

12.11. Requests can be made verbally or in writing.

12.12. 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.

13. Right to object

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

13.2. 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

13.3. 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.

13.4. 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.

13.5. 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.

13.6. 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.

13.7. 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.

13.8. 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.

13.9. 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.

13.10. Requests can be made verbally or in writing.

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

14. Rights in relation to automated decision making and profiling

14.1. 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.

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

- It is based on automated processing

14.3. 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.

14.4. 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 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.

14.5. 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.

15. Marketing and consent

15.1. 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.

15.2. 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.

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

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

16. CCTV, Photographs and Images

16.1. 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.

16.2. 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.

16.3. 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.

16.4. Clear signage will be made available to notify anyone present on site that CCTV is in operation, the purpose of CCTV, and contact details for any queries relating to the use of CCTV.

16.5. 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

16.6. 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.

16.7. 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.

17. Data Retention

17.1. Data will not be kept for any longer than is necessary. Retention periods for different types of data are outlined in the retention schedule in the ROPA.

17.2. Unrequired data will be deleted as soon as practicable.

17.3. Some educational records relating to former students or employers of the Trust may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

18. Accountability and governance

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

18.2. The Trust maintains a ROPA 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

18.3. The Trust will maintain 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.

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

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

19. Data Sharing Agreements

19.1. 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.

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

19.3. 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

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

20. "Privacy by Design" & Data Protection Impact Assessments (DPIA)

20.1. 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

20.2. Data Privacy Impact Assessments will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

20.3. 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.

20.4. 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.

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

20.6. 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

20.7. Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek it's opinion as to whether the processing operation complies with data protection obligations.

20.8. All DPIAs will be recorded on a DPIA Register, and reviewed on a regular basis

21. Data Protection Officer

21.1. 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.

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

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

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

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

22. Security

22.1. 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.

22.2. 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

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

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

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

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

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

22.8. 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.

22.9. 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.

22.10. 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.

22.11. 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.

22.12. 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.

22.13. 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.

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

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

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

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

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

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

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

22.21. Staff, Directors and Trustees must only communicate via Trust email addresses, and not use their own personal email addresses.

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

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

22.24. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

22.25. 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.

22.26. 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 for the Trust.

22.27. The Trust IT Support Manager 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 IT Support Manager also oversees the breach detection software, and will alert the DPO and Senior staff in the event of any significant potential threats.

23. Staff training

23.1. 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.

23.2. Refresher training for all staff takes place every three years.

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

24. Publication of Information

24.1. The Trust will not publish any personal information, including photographs, without the permission of the affected individual.

24.2. 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.

25. DBS Data

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

25.2. Data provided by the DBS will never be duplicated.

25.3. 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.

26. Personal data breaches

26.1. 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
- Unauthorised disclosure of personal information
- Unauthorised access to personal information
- Deletion or alteration of personal data

26.2. The Principal 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.

26.3. 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.

26.4. 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.

26.5. 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.

26.6. 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.

26.7. 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.

26.8. 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.

26.9. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate numbers of individuals affected
- The name and contact details of the DPO
- An Explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

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

27. Policy breach

27.1. 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.

27.2. 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.

28. Complaints

28.1. 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.

29. Other documents relating to this policy:

Personal Data Breach Policy
IT Acceptable Use Policy
Complaints Policy

Policy Status			
Policy Lead (Title)	Trust Data Protection Manager	**Review Period**	Every 2 years
Reviewed By	Trust Executive Team/ Board of Directors	**Equality Impact Assessment Completed (Y/N)**	N

POLICY AMENDMENTS				
Version	**Approval Date**	**Page No./Paragraph No.**	**Amendment**	**How Communicated**
Version 2		Contents		
		Pg.3, para 2.2 and 3.1		
		Pg.5, 5.3, 5.4, 5.5, 5.6		
		Pg.6, 6.7		
		Pg.7, 8.10		
		Pg.12, 15.4		
		Pg.13, 15.5, 16.8	15.5 and 16.8 removed	
		Pg.14, 17.1, 19.1, 19.2, 19.3		
		Pg.15, 19.4		
		Pg.16, 20.8		
		Pg.18, 23.2		
		Pg.19, 26.2		
		Pg.20, 27.2		