Data Protection Policy - Draft

Document Control	
Supersedes	Data Protection Policies prior to September 2021
Amendments	Small inclusions in Data Breach Form – appendix 1 as recommended by Browne Jacobson's DPO Quick Call
Process for Sign Off	Board of Trustees to approve
Review	July 2023
Responsibility	All staff – see section 5 for details

Table of Contents

1. Aims

Our Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format. As practical guidance for team members there is an accompanying Dos and Don't document.

2. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special Categories of Personal Data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

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

5.1 The Governing Board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Headteachers are responsible for ensuring there is a culture of using data with respect and ensure the policy is followed and understood in their schools. The headteacher acts as the representative of the data controller on a day-to-day basis.

5.3 Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.
The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is Jo Sands and is contactable via email on **DPO@clicmanchester.com**

5.4 All Staff

Staff are responsible for:

- collecting, storing, securing and processing any personal data in accordance with this policy
- informing the school 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 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 need help with any contracts or sharing personal data with third parties.

6. Data Protection Principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract

- The data needs to be processed so that the school can **comply with a legal obligation**

- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions

- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule/records management policy.

8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

- We need to liaise with other agencies – we will seek consent as necessary before doing this

- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us
- We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
    - The prevention or detection of crime and/or fraud
    - The apprehension or prosecution of offenders
    - The assessment or collection of tax owed to HMRC
    - In connection with legal proceedings
    - Where the disclosure is required to satisfy our safeguarding obligations
    - Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

- We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.
- Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject Access Requests and Other Rights of Individuals

9.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

  Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request either verbally or in writing, they must immediately forward it to the DPO.

9.2 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- Will ask individuals to complete the Subject Access Request form below but understand our obligation to provide information without a formal written request
- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- withdraw their consent to processing at any time
- ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- prevent use of their personal data for direct marketing
- challenge processing which has been justified on the basis of public interest
- request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- prevent processing that is likely to cause damage or distress
- be notified of a data breach in certain circumstances
- make a complaint to the ICO
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental Requests to see the Educational Record

The Trust will provide parents, or those with parental responsibility, free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. CCTV

We use CCTV in various locations around the school sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Jo Sands the Chief Operations Officer (**jsands@clicmanchester.com**).

12. Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents & carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent & carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

13. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

- Maintaining records of our processing activities, including:

    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

14. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

- Where personal information needs to be taken off site, staff must sign it in and out from the school office

- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals

- Encryption software is used to protect all portable devices, such as laptops and USB devices are not used

- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Acceptable Use Policy)

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

15. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal Data Breaches

The school will make all reasonable endeavors to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium

- Safeguarding information being made available to an unauthorised person

- The theft of a school laptop containing non-encrypted personal data about pupils.

17. Training

All staff and governors are provided with data protection training as part of their induction process. The depth of this knowledge will be assessed from time to time and data protection will also form part of continuing professional development, particularly where changes to legislation, guidance or the school's processes make it necessary.

18. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing practice outlined in this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

19. Links with other policies

This data protection policy is linked to our:

- *Data Protection Policy Dos and Don'ts*
- Freedom of information publication scheme
- *Online safety policy*
- *Policy on the acceptable use of ICT*
- *Child protection and safeguarding policy*

20. Review of Data Protection Policy

This policy will be reviewed on a bi-annual basis.

The outcomes of any breaches in the year will be reviewed and fed back to CLIC Staff to maximise on learning and development from each case.

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
2. The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
3. The DPO will alert the headteacher and the chair of governors
4. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
5. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
6. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality

- Any other significant economic or social disadvantage to the individual(s) concerned

- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

7. The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored [set out where you keep records of these decisions – for example, on the school's computer system, or on a designated software solution]

8. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

    - A description of the nature of the personal data breach including, where possible:

        - The categories and approximate number of individuals concerned

        - The categories and approximate number of personal data records concerned

    - The name and contact details of the DPO

    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

9. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

10. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

    - The name and contact details of the DPO

    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

11. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

12. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    - Records of all breaches will be retained

13. The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to Minimise the Impact of Data Breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

For Example - Sensitive information being disclosed via email (including safeguarding records):

1. *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
2. *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
3. *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
4. *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
5. *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*

6. *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.*

Appendix 1 - Reporting a Data Breach

Please only include necessary data in this report

<table>
<tr><th colspan="2">General Information</th></tr>
<tr><td>Name of person reporting the breach</td><td></td></tr>
<tr><td>Description of breach</td><td></td></tr>
<tr><td>When did the breach happen?</td><td></td></tr>
<tr><td>How was the breach discovered?</td><td></td></tr>
<tr><td>When was the breach discovered by the school (include the date / time)</td><td></td></tr>
<tr><td>Type of Breach (tick all that apply)</td><td>
<table>
<tr><td>Lost</td><td></td><td>Altered</td><td></td></tr>
<tr><td>Stolen</td><td></td><td>Disclosed or wrongly made available</td><td></td></tr>
<tr><td>Destroyed</td><td></td><td>Made available to unauthorised people</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>Categories of personal data included in the breach (tick all that apply)</td><td>
<table>
<tr><td>Data revealing racial or ethnic origin</td><td></td></tr>
<tr><td>Political opinions</td><td></td></tr>
<tr><td>Religious or philosophical beliefs</td><td></td></tr>
<tr><td>Trade union membership</td><td></td></tr>
<tr><td>Sex life data</td><td></td></tr>
<tr><td>Sexual orientation data</td><td></td></tr>
<tr><td>Gender reassignment data</td><td></td></tr>
<tr><td>Health data</td><td></td></tr>
<tr><td>Basic personal identifiers e.g. name, contact details</td><td></td></tr>
<tr><td>Identification data e.g. usernames, passwords</td><td></td></tr>
<tr><td>Economic and financial data e.g. bank details credit card numbers</td><td></td></tr>
<tr><td>Official documents e.g. driving licences</td><td></td></tr>
<tr><td>Location data</td><td></td></tr>
<tr><td>Genetic or biometric data</td><td></td></tr>
<tr><td>Criminal convictions, offences</td><td></td></tr>
<tr><td>Not yet known</td><td></td></tr>
<tr><td>Other (give details below</td><td></td></tr>
<tr><td>Had been reference to the fact there has been a CPOM referral.</td><td></td></tr>
</table>
</td></tr>
<tr><td>How many data subjects could be affected (please provide estimate per category)?</td><td>
<table>
<tr><td>Pupils</td><td></td><td>Customers</td><td></td></tr>
<tr><td>Adult Learners</td><td></td><td>Suppliers</td><td></td></tr>
<tr><td>Alumni</td><td></td><td>General Public</td><td></td></tr>
<tr><td>Parents/ Carers</td><td></td><td>Other (please specify</td><td></td></tr>
<tr><td>Employees</td><td></td><td></td><td></td></tr>
<tr><td>Trustees/Governors</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>Potential consequences of the breach</td><td></td></tr>
<tr><td>Has the subject of the data breach been informed?</td><td></td></tr>
<tr><td colspan="2">Cyber Incidents Only</td></tr>
<tr><td>Impact on IT systems (cyber incidents only)</td><td>Please describe the effect on the confidentiality, integrity and or availability of IT systems (if any)</td></tr>
</table>

<table>
<tr><td>Impact on organisation (please tick one option)</td><td><table>
<tr><td>High – the ability to provide all critical services to all users is lost</td><td></td></tr>
<tr><td>Medium – the ability to provide a critical service to some users is lost</td><td></td></tr>
<tr><td>Low – there is a loss of efficiency but all critical services can be provided to all users</td><td></td></tr>
<tr><td>Not yet known</td><td></td></tr>
</table></td></tr>
<tr><td>Recovery time</td><td><table>
<tr><td>High – the ability to provide all critical services to all users is lost</td><td></td></tr>
<tr><td>Supplemented – the recovery time can be predicted with additional resources</td><td></td></tr>
<tr><td>Extended – the recovery time cannot be predicted and need extra resources</td><td></td></tr>
<tr><td>Not recoverable – recovery from the incident is not possible e.g. sensitive data has been shared publicly</td><td></td></tr>
<tr><td>Not yet known</td><td></td></tr>
</table></td></tr>
<tr><td colspan="2">Action Plan (to be completed by the DPO)</td></tr>
<tr><td>Actions required</td><td></td></tr>
<tr><td>Communications Required</td><td>Have data subjects, other organisations (e.g. police/ LA/ ESFA/ DfE) been informed?</td></tr>
</table>

Confirmation of Action Plan	*Details of when the actions required have been carried out and their success in minimising the effect of the breach.*
Reported to the ICO Contact number 0303 123 1113 https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/	*Indicate if the breach has been reported to the ICO and if so when. Give details of the ICO contact and attach any records/ reports sent to them. If not reported to the ICO state, why this was not required.*

I confirm that the details of this breach are accurate in accordance with the information known.

Name of DPO	
Signed	
Date	
ICO Registration Number	
Date Reported to ICO	
Report Number from ICO	

<table>
<tr><td colspan="2">Cyber Incidents Only</td></tr>
<tr><td>Impact on IT systems (cyber incidents only)</td><td>Please describe the effect on the confidentiality, integrity and or availability of IT systems (if any)</td></tr>
<tr><td>Impact on organisation (please tick one option)</td><td><table>
<tr><td>High – the ability to provide all critical services to all users is lost</td><td></td></tr>
<tr><td>Medium – the ability to provide a critical service to some users is lost</td><td></td></tr>
<tr><td>Low – there is a loss of efficiency but all critical services can be provided to all users</td><td></td></tr>
<tr><td>Not yet known</td><td></td></tr>
</table></td></tr>
<tr><td>Recovery time</td><td><table>
<tr><td>High – the ability to provide all critical services to all users is lost</td><td></td></tr>
<tr><td>Supplemented – the recovery time can be predicted with additional resources</td><td></td></tr>
<tr><td>Extended – the recovery time cannot be predicted and need extra resources</td><td></td></tr>
<tr><td>Not recoverable – recovery from the incident is not possible e.g. sensitive data has been shared publicly</td><td></td></tr>
<tr><td>Not yet known</td><td></td></tr>
</table></td></tr>
<tr><td colspan="2">Action Plan (to be completed by the DPO)</td></tr>
<tr><td>Actions required</td><td></td></tr>
<tr><td>Communications Required</td><td>Have data subjects, other organisations (e.g. police/ LA/ ESFA/ DfE) been informed?</td></tr>
</table>

Confirmation of Action Plan	*Details of when the actions required have been carried out and their success in minimising the effect of the breach.*
Reported to the ICO Contact number 0303 123 1113 https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/	*Indicate if the breach has been reported to the ICO and if so when. Give details of the ICO contact and attach any records/ reports sent to them. If not reported to the ICO state, why this was not required.*

I confirm that the details of this breach are accurate in accordance with the information known.

Name of DPO	
Signed	
Date	
ICO Registration Number	
Date Reported to ICO	
Report Number from ICO	

Appendix 2 – Definitions

1) **Data Subject** is defined as a "living" individual who is the subject of Personal Data.

2) **Personal Data** is defined in the Act as information identifying a living individual ("data subject"). The School may process a wide range of personal data of pupils, their parents or guardians, as part of their operation. To qualify as personal data, the data must be biographical in a significant sense, having the data subject as its focus and affecting the data subject's privacy. Personal data includes facts, any expression of opinion about an individual and any indication of the intentions of anyone in respect of that individual. Examples of personal data are: names and addresses; bank details; academic, disciplinary, admissions and attendance records; references; and examination scripts and marks.

3) **Educational Record** is defined as information that comes from a teacher, other employee of the Local Authority or School, the pupil or their parents.

4) **Sensitive Personal Data** is defined in the Act as information in respect of racial or ethnic origin, political opinions, religious beliefs or "other beliefs of a similar nature", membership of a trade union, physical or mental health, sexual life, criminal convictions and alleged offences.

5) **Data Controller** is defined as a person or organisation that, individually or as a group, determines the purpose of holding data, and the manner of data processing.

6) **Data Processor** is defined as a person who processes data on behalf of the data controller, other than an employee of the data controller and the processing must be carried out under a contract that is made or evidenced in writing. The contract must contain obligations on the data processor to act in accordance with the instructions of the data controller.

7) **Processing** includes obtaining, holding, recording, adding, deleting, augmenting, disclosing, destroying, printing or otherwise using data.

8) **Designated Individuals** includes the following:
    - Chief Operations Officer deals with staffing matters (along with the HR Manager)
    - Headteacher and Deputy with responsibility for Pastoral Support deals with general student matters
    - Headteacher/Designated Safeguarding Person(s) deal with Child Protection matters

Appendix 3 – Subject Access Request Form

It is useful for the school to understand your request fully if you complete the attached form, however the school has an obligation to process and Subject Access Request on a verbal request.

Personal Details

1	Are you making this request for information on your own behalf? *If Yes, please go to part 2-7* *If No, please complete parts 8-11*	Yes	
		No	
2	If you are making this request for information on behalf of someone else, please state the nature of your relationship with that person.	Parent	
		Guardian	
		Legal Representative	
		Other (please specify below)	
3	If you are making this request for information on behalf of someone else please provide the following information about yourself below:		
If the applicant is not the data subject (the person we hold information on), we will always correspond with the applicant unless otherwise specified.			
4	Name		
5	Address		
	Postcode		
6	Contact Numbers	Mobile	
		Daytime	
		Evening	
7	Email Address		
		If you would prefer email contact please tick here	
Please complete the following section, providing information about the Data subject (the individual whose information is being requested)			

8	Name(s) *Include previous names*		
9	Address		
	Postcode		
10	Contact Numbers	Mobile	
		Daytime	
		Evening	
11	Email Address		
		If you would prefer email contact please tick here	
12	Date of Birth *(if under 18)*		
13	Please provide details of information you think we hold in the data subject's name. To qualify as personal data, the data must be biographical in a significant sense, having the data subject as its focus and affecting the data subject's privacy. In addition, information held in manual/paper files will only be personal data if the file is highly structured.		
	Reference numbers and departments where known ***Further details or description of information required***		

We require copies of two documents for each person to prove his or her identity, one of which should include a photograph of the person. The documents could include a passport, driving licence or any other official document, including a utility bill but showing only the name and address of the person and the name of the company, not any billing details.

If you are applying on someone else's behalf, please enclose certified proof of identity for both the data subject and yourself. Where you are acting as a legal representative or guardian of the data subject certified proof of this must also be given. If you prefer, you may provide proof with an original document by attending the School in person and bringing these documents with you.
Failure to provide these documents with your application may mean your request is refused.

After completing the application, please check to ensure that all the information you have provided is accurate and all required documents are enclosed. Sign below and return the application to:
The Chief Operations Officer, The CLIC Trust, Chorlton Park Primary School, Mauldeth Road West, Chorlton, Manchester, M21 7HH

Signed: _____

Date: _____

The CLIC Trust is committed to the principles defined in the 1998 Data Protection Act and the General Data Protection Regulation. As such, information on this document will be used only for the purposes described above. We may, however, store the data in manual or electronic form, but only for as long as we are required to do so by law.

General information about the Data Protection Act can be obtained from the Information Commissioner Information Line 0303 123 1113, or visit their website **www.ico.gov.uk**

With any queries please contact the CLIC Trust's Data Protection Officer, Jo Sands, on DPO@clicmanchester.com