Data Protection and Freedom of Information Policy

Audience:	**All Staff**
Approved:	**January 2019**
Other related policies:	**Records Management Policy, IT Acceptable Use Policy**
Policy Owner:	**Louise Wilson – Chief Executive Officer**
Policy Model:	**Compliance – all CMAT Academies use this policy**
Review:	**October 2020**
Version Number:	**1.1 (January 2019)**

Contents

1. Aims 2
2. Legislation and guidance 2
3. Definitions 2
4. The data controller 3
5. Roles and responsibilities 3
6. Data Protection principles 4
7. Collecting personal data 5
8. Sharing personal data 5
9. Subject access requests and other rights of individuals 6
10. Parental requests to see the educational record 8
11. Biometric recognition systems 8
12. CCTV 9
13. Photographs and videos 9
14. Data protection by design and default 10
15. Data security and storage of records 10
16. Disposal of records 11
17. Personal data breaches 11
18. Training 11
19. Monitoring arrangements 11
20. Freedom of Information Act 12
21. Review Process 12
22. Links with other policies 12
Appendix 1: Personal data breach procedure 13
Appendix 2: Data breach reporting template 15
Appendix 3: Subject Access Request form 16

Company Number: 07973953
Registered Office Address: Suite 4, The Lawn, Union Road, Lincoln, LN1 3BU
Telephone: 01522 849620

1. Aims

St Thérèse of Lisieux Catholic Multi Academy Trust (hereafter, STL CMAT or, the Trust) aims to ensure that all personal data collected about staff, pupils, parents, governors, directors, 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.

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 meets the requirements of the Protection of Freedoms Act 2012 when referring to the use of biometric data.

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

Company Number: 07973953
Registered Office Address: Suite 4, The Lawn, Union Road, Lincoln, LN1 3BU
Telephone: 01522 849620

	• 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

STL CMAT and the schools within the Trust process personal data relating to parents, pupils, staff, governors, directors, visitors and others, and therefore they are data controllers.
STL CMAT 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 STL CMAT, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trust Board of Directors

The Trust Board of Directors has overall responsibility for ensuring that the STL CMAT and the schools within the Trust comply with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines

Company Number: 07973953
Registered Office Address: Suite 4, The Lawn, Union Road, Lincoln, LN1 3BU
Telephone: 01522 849620

where applicable. They will provide an annual report of their activities directly to the Trust Board and, where relevant, report to the board their advice and recommendations on data protection issues. The Data Protection Controller (DPC) is the first point of contact for individuals whose data the school processes, and for the ICO who will pass the information to the DPO where necessary. Full details of the DPO's responsibilities are set out in their job description.

The DPO for the Trust is Frances Brown, the DPC for the Trust is Tamer Hodgson and is contactable via Tamer.Hodgson@stl-cmat.org.uk

5.3 STL CMAT CEO

The CEO acts as the representative of the data controller for the Trust on a day-to-day basis.

5.3 Headteacher

The Headteacher/Executive Headteacher of each school acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust and/or school of any changes to their personal data, such as a change of address
- Contacting the DPC 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 the Trust 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

Company Number: 07973953
Registered Office Address: Suite 4, The Lawn, Union Road, Lincoln, LN1 3BU
Telephone: 01522 849620

This policy sets out how the Trust 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 Trust/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 Trust/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 Trust, 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 Trust/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 where the pupil is under 13 years of age (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

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 Trust's 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

Company Number: 07973953
Registered Office Address: Suite 4, The Lawn, Union Road, Lincoln, LN1 3BU
Telephone: 01522 849620

- 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 (SAR) 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 Trust 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

Company Number: 07973953
Registered Office Address: Suite 4, The Lawn, Union Road, Lincoln, LN1 3BU
Telephone: 01522 849620

Subject access requests must be submitted in writing, either by letter or email to the DPC. 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 they must immediately forward it to the DPC. A proforma for submitting a Subject Access Request can be found in Appendix 2.

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 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.

Children aged 12 and above are generally 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 not 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:

- 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

Company Number: 07973953
Registered Office Address: Suite 4, The Lawn, Union Road, Lincoln, LN1 3BU
Telephone: 01522 849620

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.

It is expected that schools will be closed during school holidays, and therefore delays may be incurred should subject access requests be sent directly to the school. In such circumstances, requests will be passed to the DPC as soon as is practicably possible after the school holidays, and will be dealt with within one month of receipt by the DPC.

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 DPC. If staff receive such a request, they must immediately forward it to the DPC.

10. Parental Requests to See the Educational Record

There is no automatic parental right of access to the educational records in an academy setting. However, parents/carers may make a request to the school in writing to receive a copy of their child's educational record. All requests will be considered on an individual basis and reasonable fees may be charged to cover the cost of production of records.

11. Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child *(Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the*

age of 18) first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish. Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

CCTV may be used in various locations around the school site to ensure it remains safe. Where CCTV is in place, will adhere to the ICO's code of practice for the use of CCTV.
Although it is not necessary to gain individuals' permission to use CCTV, schools will make it clear where individuals are being recorded. Security cameras will be clearly visible and accompanied by prominent signs explaining that CCTV is in use.
Any enquiries about individual schools' CCTV systems should be directed to the school office.

13. Photographs and Videos

As part of School activities, photographs and record images of individuals may be taken within our schools.

Photographs/videos taken by parents/carers at school events are done so for personal use and are not covered by the Data Protection Act 2018 (GDPR). We respectfully ask that parents/carers consider the privacy rights of individuals when taking photos or videos of children other than their own (even if pictured in the background), particularly if these are to be uploaded to social media sites or other outlets.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.
Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

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

Company Number: 07973953
Registered Office Address: Suite 4, The Lawn, Union Road, Lincoln, LN1 3BU
Telephone: 01522 849620

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, unless we have gained specific consent to do so, for example, when reporting on Awards Ceremonies. Further information on how individual schools use photographs and/or videos can be obtained from the school.

14. 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/DPC, 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 data protection 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 DPC 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
- 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 the Trust, school, DPO and DPC 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

15. 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 securely stored 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
- Passwords that are at least 8 characters long containing letters and numbers are used to access Trust and school computers, laptops and other electronic devices. Staff and pupils are

Company Number: 07973953
Registered Office Address: Suite 4, The Lawn, Union Road, Lincoln, LN1 3BU
Telephone: 01522 849620

reminded to change their passwords at regular intervals in line with the Trust's ICT User Policy

- Encryption is used to protect all portable devices and removable media, such as laptops
- Staff, pupils, governors and directors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see the STL CMAT 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)

16. 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 it cannot or does not need to be rectified or updated. 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 Trust/school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal Data Breaches

STL CMAT will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, the procedure set out in appendix 1 will be followed.

When appropriate, the data breach will be reported to the ICO within 72 hours. Such breaches 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 Trust/school laptop containing non-encrypted personal data about pupils or staff

18. Training

All staff, governors and directors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust/school's processes make it necessary.

19. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy which will be reviewed **every 2 years**.

20. The Freedom of Information Act

20.1 This Act gives a general right of access to all types of 'recorded' information held by the STL CMAT. Under this Act we have two main responsibilities.

- We have a written guide available which displays the information that we hold

- We will respond to individual requests for information

20.2 The Act states that all requests for information must be made in writing to us. We will accept these in the following forms: -

- Letter
- Email

20.3 The following information must be included

- The requestor's full name
- An address for correspondence, (this can be a postal or email address)
- A clear description of the information required.

20.4 We will respond to requests for information within 20 school days. If further clarification is required, our staff will write to the requestor and the request will be temporarily placed on hold until sufficient information is available to begin processing the request

20.5 We will not charge those making a Freedom of Information request. In some circumstances we may be allowed to charge an appropriate fee for complying with some requests for information.

21. Review Process

21.1 Under section 45 of the Act a requestor can ask for a formal review of any refusal notice and/or the administration of their request. The request for a review must be made in writing and received by the Chair of Directors within 40 working days of the alleged failure to comply with the Act.

22.2 On receipt of a request to review the Chair of Directors and CEO will conduct a full assessment and aim to respond within 20 school days.

22.3 If upon following this process the requestor remains dissatisfied they should then contact the Information Commissioner's Office for advice.

22. Links with other policies

This data protection policy is linked to our:

- Records Management Policy
- IT User Policy

Appendix 1: Personal Data Breach Procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPC
- The DPC/DPO will investigate the report and determine whether a breach has occurred. To decide, the DPC/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
- The DPC will alert the Headteacher/Executive Headteacher
- The DPC/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)
- The DPC/DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPC/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 DPC/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 DPC/DPO must notify the ICO.
- The DPC/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 in the Data Protection folder on the CMAT One Drive
- Where the ICO must be notified, the DPC/DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPC/DPO will set out:
    - A description of the nature of the personal data breach including, where possible:

Company Number: 07973953
Registered Office Address: Suite 4, The Lawn, Union Road, Lincoln, LN1 3BU
Telephone: 01522 849620

        - 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
- If all the above details are not yet known, the DPC/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 DPC/DPO expects to have further information. The DPC/DPO will submit the remaining information as soon as possible
- The DPC/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 DPC/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 DPC/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
- The DPC/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
- The DPC/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 stored in the Data Protection folder on the CMAT One Drive.
- The DPC/DPO and CEO/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.

Appendix 2: Data Breach Reporting Template

In the event of a data breach, please complete the form below and return to the Data Protection Controller without delay.

Date of breach	
Person responsible for dealing with breach	
Description of breach	
Which data subjects are involved? e.g. pupils	
Reported by	
Is this high risk? Has it been reported to ICO?	
Date reported to data subjects	
Actions taken	
Lessons learned e.g. preventative actions	
Notes	
Actions approved by/date	

Company Number: 07973953
Registered Office Address: Suite 4, The Lawn, Union Road, Lincoln, LN1 3BU
Telephone: 01522 849620

Appendix 2: Subject Access Request Template

SUBJECT ACCESS REQUEST FORM

The General Data Protection Regulations (GDPR) provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to see your data. You will also need to **confirm your identity** if any of your details provided differ from those we have.

Proof of identity:
Before we can disclose personal data you may be required to provide proof of your identity, if this is the case we will contact you. If requested, proof of your identity should include a copy of two documents such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g. bank statement, recent utilities bill or council tax bill. The documents should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Retention Period:
This request will be kept on file for a 12-month period at which point it will be securely destroyed. We keep this information to assess if this request or any subsequent requests are manifestly unfounded, repetitive or excessive. Upon confirming your identity, any documents relating to your identity will be securely destroyed and a note made of this form.

Section 1 – Data Subject
Please fill in your details (the data subject). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title:	
Surname:	
Forename(s)	
Date of Birth:	
Address: **Postcode:**	
Email Address:	
School (if applicable):	

Company Number: 07973953
Registered Office Address: Suite 4, The Lawn, Union Road, Lincoln, LN1 3BU
Telephone: 01522 849620

Section 2 – Information Requested

Please tell us what information or records you would like to use to disclose. Please be as specific as possible. We reserve the right to ask for clarification if the initial request broad in nature.

Details:
Employment Records ☐ If you are now, or have been employed by St Thérèse of Lisieux Catholic Multi Academy Trust and are seeking personal information in relation to your employment, please provide details of your dates of employment.

Section 3 – Authorised Person

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e. the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title:	
Surname:	
Forename(s)	
Date of Birth:	
Address:	

Postcode:	
Email Address:	
Daytime Telephone Number:	
What is your relationship to the data subject? (e.g. Parent/Carer, Legal Representative)	
I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject: Letter of authority ☐ Lasting or Enduring Power of Attorney ☐ Evidence of parental responsibility ☐ Other (give details): ☐	

Section 4 – Declaration

Data Subject I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that St Thérèse of Lisieux Catholic Multi Academy Trust is obliged to confirm proof of identity/authority and it may be necessary to obtain further information in order to comply with this subject access request.	
Name:	
Signature:	**Date:**

OR

Authorised Person – Declaration (if applicable): I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that St Thérèse of Lisieux Catholic Multi Academy Trust is obliged to confirm proof of identity/authority and it may be necessary to obtain further information in order to comply with this subject access request.	
Name:	

Signature:	**Date:**

I wish to:

Receive the information in electronic format ☐
(if files are too large to do so, other arrangements will be made)

Receive the information by post* ☐

Collect the information in person ☐

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity to:

SAR Data Protection Controller, Tamer Hodgson
Suite 4, The Lawn,
Union Road, Lincoln
LN1 3BU

OR

Tamer.Hodgson@stl-cmat.org.uk

For Office Use Only

Date received	
Proof of Identity Required	
Proof of Identity Received & Date	
Additional Information Requested	
Date SAR Sent	
Identity Documents Destroyed on	