Data Breach Notification Policy

February 2023

Our Lady of Lourdes Catholic Multi-Academy Trust - Company Number: 7743523
Registered Office: 1st Floor, Loxley House, Riverside Business Park, Tottle Road, Nottingham NG2 1RT

Contents

Trust Mission Statement

We are a partnership of Catholic schools and our aim is to provide the very best Catholic education for all in our community and so improve life chances through spiritual, academic and social development.

We will achieve this by:

- Placing the life and teachings of Jesus Christ at the centre of all that we do
- Following the example of Our Lady of Lourdes by nurturing everyone so that we can all make the most of our God given talents
- Working together so that we can all achieve our full potential, deepen our faith and know that God loves us
- Being an example of healing, compassion and support for the most vulnerable in our society

1 Corinthians *14: 40 (GNT)*

Everything must be done in a proper and orderly way

1 Policy Statement

1.1 [Trust/School] is committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.2 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.3 All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

2 About this policy

2.1 This policy informs all of our **workforce** on dealing with a suspected or identified data security breach.

2.2 In the event of a suspected or identified breach, [Trust/School] must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring.

2.3 Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible.

2.4 The [Trust/School] must also comply with its legal and contractual requirements to notify other organisations including the Information Commissioners Office ("the ICO") and where appropriate **data subjects** whose **personal data** has been affected by the breach. This includes any communications with the press.

2.5 Failing to appropriately deal with and report data breaches can have serious consequences for the [Trust/School] and for **data subjects** including:

2.5.1 identity fraud, financial loss, distress or physical harm;

2.5.2 reputational damage to [Trust/School]; and

2.5.3 fines imposed by the ICO.

3 Definition of data protection terms

3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in Annex 2 to this policy.

4 Identifying a Data Breach

4.1 A data breach is a **breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data**.

4.2 This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:

4.2.1 Leaving a mobile device on a train;

4.2.2 Theft of a bag containing paper documents;

4.2.3 Destruction of the only copy of a document; and

4.2.4 Sending an email or attachment to the wrong recipient; and

4.2.5 Using an unauthorised email address to access personal data; and

4.2.6 Leaving paper documents containing personal data in a place accessible to other people.

5 Internal Communication

Reporting a data breach upon discovery

5.1 If any member of our **workforce** suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our **workforce**, a **data processor**, or any other individual) then they must contact the Data Protection Officer ("the DPO"), School GDPR Lead & Headteacher immediately at:

DPO Tamer Robson DPO@ololcatholicmat.co.uk

All Saints' Catholic Voluntary Academy – GDPR Lead Jane Ellis-Laycock ellis-laycock.j@allsaints.notts.sch.uk

All Saints' Catholic Voluntary Academy – Headteacher Carlo Cuomo cuomo.c@allsaints.notts.sch.uk

5.2 The data breach may need to be reported to the ICO, and notified to **data subjects**. This will depend on the risk to **data subjects**. The DPO must always be consulted in making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

5.3 If it is considered to be necessary to report a data breach to the ICO then the Trust must do so within 72 hours of discovery of the breach.

5.4 The [Trust/School] may also be contractually required to notify other organisations of the breach within a period following discovery.

5.5 It is therefore critically important that whenever a member of our **workforce** suspects that a data breach has occurred, this is reported internally to the DPO, School GDPR Lead & Headteacher immediately.

5.6 Members of our **workforce** who fail to report a suspected data breach could face disciplinary or other action.

Investigating a suspected data breach

5.7 In relation to any suspected data breach the following steps must be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

***Breach minimisation**:*

5.8 The first step must always be containment of the breach, and to identify how the data breach occurred, the extent of the data breach, and how this can be minimised. The focus will be on containing any data breach, and recovering any **personal data**. Relevant departments must be involved, such as IT, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:

5.8.1 remote deactivation of mobile devices (if possible);

5.8.2 shutting down IT systems (if possible);

5.8.3 contacting individuals to whom the information has been disclosed and asking them to delete the information; and

5.8.4 recovering lost data.

***Breach investigation**:*

5.9 When the [Trust/School] has taken appropriate steps to minimise the extent of the data breach it must commence an investigation as soon as possible to understand how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from occurring.

5.10 Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:

5.10.1 what data/systems were accessed;

5.10.2 how the access occurred;

5.10.3 how to fix vulnerabilities in the compromised processes or systems;

5.10.4 how to address failings in controls or processes.

5.11 Other steps are likely to include discussing the matter with individuals involved to appreciate exactly what occurred and why, and reviewing policies and procedures.

***Breach analysis**:*

5.12 In order to determine the seriousness of a data breach and its potential impact on **data subjects**, and so as to inform the [Trust/School] as to whether the data breach should be reported to the ICO and notified to **data subjects**, it is necessary to analyse the nature of the data breach.

5.13 Such an analysis must include:

5.13.1 the type and volume of **personal data** which was involved in the data breach;

5.13.2 whether any **special category personal data** was involved;

5.13.3 the likelihood of the **personal data** being accessed by unauthorised third parties;

5.13.4 the security in place in relation to the **personal data**, including whether it was encrypted;

5.13.5 the risks of damage or distress to the **data subject**.

5.14 The breach notification form annexed to this policy must be completed in every case of a suspected breach, and retained securely, whether or not a decision is ultimately made to report the data breach. This will act as evidence as to the considerations of the [Trust/School] in deciding whether or not to report the breach.

6 External communication

6.1 Related external communication is to be managed and overseen by the DPO in liaison with the School GDPR Lead & Headteacher.

Law Enforcement

6.2 The DPO in liaison with the School GDPR Lead & Headteacher will assess whether the data breach incident requires reporting to any law enforcement agency, including the police. This will be informed by the investigation and analysis of the data breach, as set out above.

6.3 DPO in liaison with the School GDPR Lead & Headteacher shall coordinate communications with any law enforcement agency.

Other organisations

6.4 If the data breach involves **personal data** which we process on behalf of other organisations, then we may be contractually required to notify them of the data breach.

6.5 The [Trust/School] will identify as part of its investigation of the data breach whether or not this is the case and any steps that must be taken as a result.

Information Commissioner's Office

6.6 If [Trust/School] is the **data controller** in relation to the **personal data** involved in the data breach, which will be the position in most cases, then the [Trust/School] has 72 hours to notify the ICO if the data breach is determined to be notifiable.

6.7 A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The [DPO] will make an assessment of the data breach against the following criteria taking into account the facts and circumstances in each instance:

6.7.1 the type and volume of **personal data** which was involved in the data breach;

6.7.2 whether any **special category personal data** was involved;

6.7.3 the likelihood of the **personal data** being accessed by unauthorised third parties;

6.7.4 the security in place in relation to the **personal data**, including whether it was encrypted;

6.7.5 the risks of damage or distress to the **data subject**.

6.8 If a notification to the ICO is required, then see part 7 of this policy below.

[In the vast majority of cases the [Trust/School] will be data controller, however if the [Trust/School] is ever acting only as data processor then on identifying any breach it should only report the matter to the organisation which is the data controller, whose responsibility it is to then investigate the breach, though cooperation may be required from the [Trust/School].]

Other supervisory authorities

6.9 If the data breach occurred in another country or involves data relating to data subjects from different countries, then the [DPO] will assess whether notification is required to be made to supervisory authorities in those countries.

Data subjects

6.10 When the data breach is likely to result in a high risk to the rights and freedoms of the **data subjects** then the **data subject** must be notified without undue delay. This will be informed by the investigation of the breach by the [Trust/School].

6.11 The communication will be coordinated by the DPO in liaison with the School GDPR Lead & Headteacher and will include at least the following information:

6.11.1 a description in clear and plain language of the nature of the data breach;

6.11.2 the name and contact details of the DPO/School GDPR Lead/Headteacher;

6.11.3 the likely consequences of the data breach;

6.11.4 the measures taken or proposed to be taken by [Trust/School] to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

6.12 There is no legal requirement to notify any individual if any of the following conditions are met:

6.12.1 appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);

6.12.2 measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;

6.12.3 it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.

6.13 For any data breach, the ICO may mandate that communication is issued to **data subjects**, in which case such communication must be issued.

Press

6.14 Staff shall not communicate directly with the press and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the DPO.

6.15 Data breach-related press enquiries shall be directed to the DPO.

7 Producing an ICO Breach Notification Report

7.1 All members of our **workforce** are responsible for sharing all information relating to a data breach with the DPO/School GDPR Lead/Headteacher, which will enable the annexed Breach Notification Report Form to be completed.

7.2 When completing the attached Breach Notification Report Form all mandatory (*) fields must completed, and as much detail as possible should be provided.

7.3 The DPO may require individuals involved in relation to a data breach to each complete relevant parts of the Breach Notification Form as part of the investigation into the data breach.

7.4 If any member of our **workforce** is unable to provide information when requested by the DPO then this should be clearly reflected in the Breach Notification Form together with an indication as to if and when such information may be available.

7.5 In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

7.6 The ICO requires that the Trust send the completed Breach Notification Form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

8 Evaluation and response

8.1 Reporting is not the final step in relation to a data breach. The [Trust/School] will seek to learn from any data breach.

8.2 Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of our **workforce** to reinforce good practice, or providing additional training, or may in more serious cases require new technical systems and processes and procedures to be put in place.

Date Issued	Feb 2023
Date of Review	Feb 2026
Reviewer	OLoL Audit & Risk Committee / OLoL Exec Board
Author	Browne Jacobson template – edited by Tamer Robson

ANNEX 1 – ICO Breach Notification Report

1. Organisation Details

Name of Organisation	
Data controller's registration number (if applicable).	Z2843072
DPO	Tamer Robson Tel: 0115 851 5454
School Contact Details	Name: Tel:

2. Details of the data protection breach

Set out the details of the breach and ensure that all mandatory (*) fields are completed.

(a) * Please describe the incident in as much detail as possible. (b) * When did the incident happen?

(c) * How did the incident happen?

(d) If there has been a delay in reporting the incident to the ICO please explain your reasons for this.

(e) What measures did the organisation have in place to prevent an incident of this nature occurring?

- The Trust has the following GDPR-related policies in place:
  - Data Protection Policy
  - Data Breach Policy & Procedure
  - Safeguarding Policy
  - Staff Code of Conduct Policy
  - Compulsory online GDPR Awareness Training for all staff
  - Compulsory online Safeguarding Training for all staff

(f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

OLoL Data Protection Policy – July 2021

13. Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.
We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

Security procedures include:
Entry controls. Any stranger seen in entry-controlled areas should be reported to the Headteacher/Principal of the school.
Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in

accordance with the Information Commissioner's Office guidance on the disposal of IT assets.
Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off or lock their PC when it is left unattended.
Working away from the school premises – paper documents. Wherever possible, employees should avoid taking paper documents containing personal data away from the Trust/school premises.
Working away from the school premises – electronic working. Where possible, confidential data should be accessed via Trust owned devices, however, there may be occasions where the [CEO/Trust IT Director/Headteacher (insert others)] may authorise use of personal devices such as reviewing email on a personal phone. Where this is authorised, the Trust/School will enforce security measures on the device, or on the access (for example, multi-factor authentication, PIN code and encryption requirements on mobile device, selective wipe of email). This is to ensure that data remains secure.

To supplement this, any data transfer must occur within Trust owned systems – for example, but not limited to, use of Office 365/Google Workspace. Trust data must not be transferred using personal services or personal email. Where confidential data is accessed on a Trust owned device, this may also include access to onsite via Virtual Private Network. As a last resort, Encrypted USB sticks may be used to transfer confidential data, however all other avenues of data transfer must be exhausted before use and any confidential information should be removed as soon as practicable.

Document printing. Documents containing personal data must be collected immediately from printers and not left on photocopiers and where possible, print release should be used to ensure documents do not print until you are at the printing location.

Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

15. Disclosure and sharing of personal information
We may share personal data that we hold about data subjects, and without their consent, with other organisations. Such organisations include the Department for Education, [and / or Education and Skills Funding Agency "ESFA"], Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

The School/Trust will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

Further detail is provided in our Schedule of Processing Activities.

OLoL Safeguarding Policy – 2022, Keeping Children Safe in Education 2022 – read annually by staff

OLoL Staff Code of Conduct Policy – Dec 2021

Confidentiality and protection of data

9.1 Members of staff may have access to confidential information about pupils/students, colleagues or other matters relating to the School/CMAT. This could include personal and sensitive data, for example information about a pupil's/student's home life. Employees should never use this information to their own personal advantage, or to humiliate, intimidate or

embarrass others. Employees should never disclose this information unless this is in the proper circumstances and with the proper authority.

9.2 If an employee is ever in doubt about what information can or can't be disclosed they should speak to the Headteacher/their Line Manager.

9.3 The School/CMAT holds and processes data that is protected under the Data Protection Act 1998. Employees are expected to comply with the School/CMAT's systems for collecting, storing and using data. If any employee becomes aware that data is at risk of compromise or loss, or has been compromised or lost they must report it immediately to the Headteacher or, in the case of a centrally based CMAT role, their Line Manager.

9.4 Employees must ensure that they have read and understood all of our polices that relate to data including our IT policies.

3. Details of the Personal Data placed at risk

Set out the details of the personal data placed at risk as a result of the breach and ensure that all mandatory (*) fields are completed.

(a) * What personal data has been placed at risk? Please specify if any financial or special category (sensitive) personal data has been affected and provide details of the extent.

(b) * How many individuals have been affected?

(c) * Are the affected individuals aware that the incident has occurred?

(d) * What are the potential consequences and adverse effects on those individuals?

(e) Have any affected individuals complained to the School / Trust about the incident?

4. Containment and recovery

Set out the details of any steps the School / Trust has taken to contain the breach and/or to recover the personal data and ensure that all mandatory (*) fields are completed.

(a) * Has the [Trust/School] taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

(b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

(c) What steps has the [Trust/School] taken to prevent a recurrence of this incident?

5. Training and guidance

Set out the details of any steps the [Trust/School] has taken to contain the breach and/or to recover the personal data and ensure that all mandatory (*) fields are completed.

(a) As the data controller, does the [Trust/School] provide its staff with training on the requirements of Data Protection Legislation? If so, please provide any extracts relevant to this incident here.

Please see 2 e & f above

(b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

Yes, training is mandatory and undertaken on an annual basis. Please see 2 e & f above

(c) As the data controller, does the [Trust/School] provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

Please see 2 e & f above

6. Previous contact with the ICO

(a) * Have you reported any previous incidents to the ICO in the last two years?

YES / NO

(b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

(a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.

(b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.

(c) Have you informed any other regulatory bodies about this incident? If so, please provide details.

(d) Has there been any media coverage of the incident? If so, please provide details of this.

This form was completed on behalf of [Trust/School] by:

Name:…….

Role:……..

Date and Time:……..

ANNEX 2 - DEFINITIONS

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by [School/Trust] such as staff and those who volunteer in any capacity including Governors [and/or Trustees / Members/ parent helpers]