Data Breach Response Plan for St Francis of Assisi Catholic Academy Trust

St. Francis of Assisi Catholic Academy Trust

Signed off by: Trust Board

Date from: November 2024

Review Date: November 2025

Contents

Data Breach Response Plan for St Francis of Assisi Catholic Academy Trust

1. **Introduction**

1.1 St Francis of Assisi Catholic Academy Trust has implemented appropriate technical and organisational measures to avoid data security breaches. However, in the event that a data security breach happens, we recognise that it is important that the Trust and its Academies are able to detect it and react swiftly and robustly in order to mitigate any risks to data subjects and to comply with our obligations under the UK General Data Protection Regulation ('UK GDPR').

1.2 This Data Breach Response Plan sets out how we will respond to any suspected or actual data breaches and should be read alongside our Data Protection Policy.

1.3 The UK GDPR requires the Trust to report 'notifiable breaches' without undue delay and, where feasible, not later than 72 hours after having become aware of it. Notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals. In the event that a report is not made within 72 hours, the Trust is required to provide the reasons for the delay in reporting it to the ICO.

1.4 If there is deemed to be a "high risk" to the rights and freedoms of individuals following a personal data breach, the Trust is also required to notify the individuals affected by the breach. However, in the interests of transparency, the Trust recognises that on some occasions it will be appropriate to notify affected individuals, even if we are not legally obliged to do so.

1.5 If the Trust fails to report a notifiable personal data breach, we are at risk of receiving a sanction from the ICO, which may include a fine. Aside from our desire to avoid receiving any sanctions, the purpose of this Data Breach Response Plan is to ensure that we protect the Personal Data of our stakeholders and minimise any risks to them following a breach.

1.6 The Trust and its Academies will ensure that staff are aware of and are trained on this Data Breach Response Plan to ensure it is effective should a data security incident occur. In particular, the Data Response Team identified below, must receive training on their roles and responsibilities should a breach occur. For example, our in-house IT team at St Mary's Catholic School and our external IT support for our Primary Schools must be trained on how to identify if the security of our IT systems have been compromised and the steps that need to be taken to respond to a breach, for example, if data on a remote device needs to be wiped.

1.7 We rely on our staff to be alert to the risk of data security breaches and to follow the procedures set out in this Data Breach Response Plan to ensure that we can react promptly in the event that a breach or suspected breach occurs. Any member of staff who becomes aware of a suspected or actual personal data breach must follow the escalation procedures set out below. Failure to comply with these procedures may be a disciplinary issue.

The Trust's DPO is Dominic Tisi - d.tisi@stfrancistrust.net.

Please see the Glossary at the end of this privacy notice for definitions of key terms.

2. **What is a personal data breach?**

2.1 The legal definition of a personal data breach is, "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

2.2 A data security breach covers more than the simple misappropriation of data and may occur through incidents, such as:

2.2.1 Loss or theft of data or equipment;

2.2.2 People gaining inappropriate access to personal data;

2.2.3 A deliberate attack on systems;

2.2.4 Equipment failure;

2.2.5 Human error;

2.2.6 Acts of God (for example, fire or flood);

2.2.7 Malicious acts such as hacking, viruses or deception.

2.3 Examples of common personal data breaches include:

2.3.1 Sending an email to the wrong recipient;

2.3.2 Losing a USB stick which contains personal data;

2.3.3 Having a laptop stolen which contains personal data;

2.3.4 Sending a letter or email to the wrong address;

2.3.5 Network, phishing, malware or other cyber security incidents.

2.4 A security incident resulting in personal data being made unavailable for temporary period is also a type of breach, as the lack of access to the data could have a significant impact on the rights and freedoms of data subjects, for example, if our IT system goes down. This type of breach should be recorded in the Trust's Data Breach Log set out in Appendix 1 so that we keep records of all such incidents. Individual Schools should also have their own Data Breach Log where such incidents are recorded. However, depending on the circumstances of the breach, it may or may not require notification to the ICO and communication to affected individuals.

2.5 Where personal data is unavailable due to planned system maintenance being carried out, this should not be regarded as a 'breach of security'.

3. **Understanding the risk to the rights and freedoms of individuals**

3.1 A breach can potentially have a number of consequences for individuals, which can result in physical, material, or non-material damage. This can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals.

3.2 When assessing the risk to individuals, the DPO must consider the following factors:

3.2.1 the type of breach;

3.2.2 the nature, sensitivity, and volume of personal data;

3.2.3 ease of identification of individuals;

3.2.4 severity of consequences for individuals;

3.2.5 special characteristics of the individual;

3.2.6 special characteristics of the data controller; and

3.2.7 the number of affected individuals.

4. Timescales for reporting a breach

4.1 The Trust and its Academies are required to report a notifiable breach without undue delay and, where feasible, not later than 72 hours after having become aware of it.

4.2 It is likely that the Trust and its Academies will be deemed as having become "aware" of a breach when we have a reasonable degree of certainty that a security incident has occurred which has led to personal data being compromised. The UK GDPR expects us to ascertain whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place. This puts an obligation on us to ensure that we will be "aware" of any breaches in a timely manner so that we can take appropriate action.

4.3 While some breaches may be obvious, in other cases we may need to establish whether personal data has been compromised. In such circumstances, we will investigate promptly in accordance with the procedures below to determine whether a breach has happened which, in turn, will enable us to decide if remedial action is needed and if the breach needs to be notified to the ICO and the affected data subjects.

4.4 It is possible that we may not have established all of the relevant facts following a data security breach or completed our investigation within 72 hours. However, in the event that the Trust determines that a breach has taken place and that it needs to be notified to the ICO, a report should be made within 72 hours with the information held at that point in time. In these circumstances, the report to the ICO should explain that further information will be provided as and when it is available.

4.5 It is possible that some breaches may come to the attention of a member of staff or may be flagged up by our IT systems. However, it is also possible that we may be notified about breaches by third parties, such as the people who are affected by the breach, a data processor or by the media.

4.6 In the event that we investigate a suspected breach and we are able to establish that no actual breach has occurred, the Data Breach Log in Appendix 1 must still be completed so that we can keep records of 'near misses' or other weaknesses in our systems and procedures in order to continuously review and improve our processes.

5. Response plan

5.1 A member of staff within an academy who becomes aware of a suspected or actual data security breach must inform the Headteacher or the Academy Data Protection Manager or the DPO of the Trust by email without delay. The email address for contacting the DPO is outlined in section 1.7 and the email account is regularly reviewed by the DPO. The Academy Data Protection Lead should be copied in to the email to the DPO.

5.2 A member of staff within the central team at the Trust who becomes aware of a suspected or actual data security breach must inform the DPO by email without delay.

5.3 If a member of staff is unsure if a breach has happened, the above procedures must still be followed without delay so that the suspected breach can be investigated in order to establish whether a breach has happened and, if so, whether it needs to be notified to the ICO or the data subjects.

5.4 The Academy Data Protection Lead will then be responsible for assessing whether the breach or suspected breach needs to be formally escalated to the DPO. If the Academy Data Protection Lead decides not to escalate it to the DPO, the Data Breach Log in Appendix 1 must be completed as accurately as possible, including the reasons why the incident does not need to be escalated to the DPO. The Data Breach Log should be emailed to the DPO without delay for record keeping purposes.

5.5 If the Academy Data Protection Lead decides to escalate a breach or suspected breach to the DPO, they must do so without delay. Where possible, the Data Breach Log in Appendix 1 must be completed with as much information as possible and emailed to the DPO. However, if it is not convenient or practicable to complete the Data Breach Log, the report can be made by setting the information out in an email.

5.6 Once a breach or suspected breach has been reported to the DPO, the DPO must commence an investigation and assess whether he / she has sufficient information to identify next steps. The purpose of the investigation is to:

5.6.1 establish if a breach has happened;

5.6.2 establish the nature and cause of the breach;

5.6.3 establish the extent of the damage or harm that results or could result from the breach;

5.6.4 identify the action required to stop the data security breach from continuing or recurring; and

5.6.5 mitigate any risk of harm that may continue to result from the breach.

5.7 The DPO should contact the Academy Data Protection Lead if further information is required. The DPO may also need to speak to the member of staff who first reported the breach or suspected breach.

5.8 During the course of his or her investigation, the DPO should consider whether to involve the Academy's Data Breach Response Team which consists of:

5.8.1 Headteacher

5.8.2 Academy Data Protection Lead

5.9 If the DPO is unavailable for any reason, for example, the DPO is on annual leave, on sickness absence or is otherwise not available to respond to the data breach, then the Academy Data Protection Lead must fulfil the responsibilities of the DPO set out in this Data Breach Response Plan. The Academy Data Protection Lead must have access to the email account identified above to which data breaches are reported.

5.10 If the DPO decides to involve the Data Breach Response Team, the above individuals should be copied into email correspondence and provided with regular updates on the investigation and response to the incident. The roles and responsibilities of the Data Breach Response Team are as follows: Headteacher and Academy Data Protection Lead.

5.11 The DPO should take steps to identify any risks arising from the personal data breach:

5.11.1 Consider obtaining specialist legal advice;

5.11.2 Confirm the amount, sensitivity and type of information in question;

5.11.3 Identify what security measures were in place when the breach occurred as well as what measures have been put in place following it;

5.11.4 Confirm who has been put at risk and assess the potential harm resulting from the breach;

5.11.5 Consider the additional consequences of the breach including loss of reputation, loss of business, liability for fines or contractual breaches.

5.12 The DPO should consider whether input is required from the Academies IT or HR support team in order to further investigate the incident, including the extent of the incident and whether any steps need to be taken to contain any breach. As the Trust and its Academies has external HR and IT support, the relevant contact details are set out in Appendix 2.

5.13 Depending on the circumstances, the DPO should also consider whether the Trust's Risk Protection Arrangement should be notified in accordance with policy terms, whether legal advice is required and if the incident needs to be reported to the Police. The DPO should also consider if specialist IT support is required in order to contain and manage a breach and whether the Trust's PR advisors should be engaged if it is likely that we will need to communicate internally and / or externally with our stakeholders regarding the breach or suspected breach. The contact details for the organisations referred to in this paragraph are set out in Appendix 2.

5.14 If the breach or suspected breach has occurred at one of our Data Processors, the DPO must liaise with the Data Processor to obtain as much information as possible about the extent of the breach or suspected breach and any steps being taken to mitigate any risk to data subjects. It remains the Trust's responsibility to decide whether to report any such breach to the ICO within 72 hours.

5.15 The same requirement applies if the breach or suspected breach is reported to us by a joint Data Controller though in this case we need to establish with the joint Data Controller who is going to report the breach to the ICO and the data subjects if such notification is required.

5.16 Depending on the timescales as to when a member of staff originally became aware of a breach, the DPO must be mindful of the requirement to notify the ICO without delay and within 72 hours unless it is unlikely to result in a risk to the rights and freedoms of individuals. As stated above, it is therefore possible that a data security breach may need to be reported to the ICO before the Trust has fully investigated or contained the breach. A report to the ICO must contain the following information:

5.16.1 the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned;

5.16.2 the name and contact details of the DPO or other contact point where more information can be obtained;

5.16.3 the likely consequences of the personal data breach;

5.16.4 the measures taken or proposed to be taken by the Trust to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.17 The DPO is not required to provide precise details in the report to the ICO if this information is not available and an updated report can be made as and when further details come to light. Such further information may be provided in phases without undue further delay. The DPO should inform the ICO if the Trust does not yet have all the required information and if further details will be provided later on.

5.18 If a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred, this information could then be added to the information already given to the ICO and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

5.19 In the event that a notifiable breach is not reported to the ICO within 72 hours, a report should be made without delay with the reasons for the delay.

5.20 If the DPO concludes that a referral to the ICO is required and also concludes that there is likely to be a high risk to the rights and freedoms of individuals resulting from the data security breach then the data subjects affected by the breach must also be notified without undue delay. The DPO must liaise with the Headteacher and the Chief Executive Officer in relation to how the issue should be communicated to the relevant stakeholders. The DPO will need to consider which is the most appropriate way to notify affected data subjects, bearing in mind the security of the medium as well as the urgency of the situation. The notice to the affected individuals should contain the following information:

5.20.1 description of the nature of the breach;

5.20.2 the name and contact details of the DPO or other contact point;

5.20.3 a description of the likely consequences of the breach; and

5.20.4 a description of the measures taken or proposed to be taken by the Trust to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Given that a large number of our stakeholders are children, if a data breach affects our pupils, it is likely that the above information will need to be given to parents / carers if the affected pupils are aged 12 or under. If the affected pupils are aged 13 or over, the pupils should be informed and it may also be appropriate to notify parents / carers, depending on the circumstances and the nature of the personal data which has been compromised.

5.21 If the DPO decides to notify data subjects about a breach, the notification should at the very least include a description of how and when the breach occurred and what data was involved. Details of what the organisation has already done to respond to the risks posed by the breach should also be included. The Trust should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised.

5.22 Particular consideration will be given to whether there are any parties that we are legally or contractually obliged to notify (e.g. insurers, regulator).

5.23 The DPO must complete the Data Breach Log in Appendix 1 before making the referral to the ICO and keep it under review as and when further information comes to light.

5.24 In certain circumstances, where justified, and on the advice of law-enforcement authorities, the Trust may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.

5.25 Even if the DPO initially decides not to communicate the breach to the affected data subjects, the ICO can require us to do so, if it considers the breach is likely to result in a high risk to individuals.

5.26 In the event that the DPO concludes that it is not necessary to refer the breach to the ICO, the DPO must still complete the Data Breach Log in Appendix 1 and clearly set out the reasons why

the DPO is satisfied that a referral is not required. The DPO must keep the decision under review and be prepared to make a referral to the ICO if any circumstances change or if any information comes to light which means that a referral should be made.

5.27 Once the breach has been contained and action taken to stop or mitigate the breach, the DPO must then review the incident and identify any steps which need to be taken in order to prevent a similar breach occurring in future. This may also include whether any disciplinary action is required against any members of staff or pupils.

5.28 As part of the review process, the DPO should undertake an audit which should include a review of whether appropriate security policies and procedures were in place and if so, whether they were followed. The audit should include an assessment of any ongoing risks associated with the breach and evaluate the Trust and its Academies response to it and identify any improvements that can be made. The review should also consider the effectiveness of this Data Breach Response Plan and whether any amendments need to be made to it.

5.29 Where security is found not to be appropriate, the DPO should consider what action needs to be taken to raise data protection and security compliance standards and whether any staff training is required.

5.30 Where a data processor caused the breach, the DPO should consider whether adequate contractual obligations were in place to comply with the UK GDPR and if so, whether the data processor is in breach of contract.

6. School holidays

6.1 The Trust recognises that there are times throughout the year when our ability to identify and respond to a breach swiftly and robustly may be impeded because the Trust and its academies are closed and has very limited staff available during school holidays. A breach may still occur during these periods and we will implement the following steps to mitigate any risk caused if a breach happens during the school holidays:

6.1.1 The DPO email address will be made available to staff and will be available on our website and in our privacy notices so that a member of staff can be contacted should an incident occur. This email address will be monitored regularly by the assigned member of staff.

6.1.2 The DPO will have the contact details for the Headteachers, the Chief Executive Officer, our IT support, our legal advisors and our insurers so that action can be taken without delay should a breach occur.

6.1.3 The DPO should follow the steps set out above as best as he / she can in the circumstances. In particular, this should include reporting notifiable breaches to the ICO within 72 hours and, if required, the affected individuals. The report to the ICO should state that the Trust is closed and has very limited staff available due to the school holidays and, depending on the circumstances, advice should be sought from the ICO on the steps the Trust and its Academies should take to mitigate any risks.

7. Review

7.1 This Data Breach Response Plan will be kept under review by the DPO and may be revised to reflect good practice or changes to our organisational structure. The Plan will be reviewed annually and approved by the Trust Board.

Appendix 1 – Data Breach Log for St Francis of Assisi Catholic Academy Trust

This Data Breach Log must be completed by a suitably trained person following any reports of a security breach or suspected breach involving personal data. Staff must follow the Trust's Data Breach Response Plan following notification of a breach or suspected breach. In the event you are unsure whether to notify the ICO and the data subjects, you should obtain legal advice without delay as the ICO must be informed about notifiable breaches within 72 hours.

You may find it easier to set up an Excel spreadsheet to include some or all of the suggested headings below.

Information	Response
Date and time this record was completed	
Name of person completing this record	
General description of the breach	
Name and job title of person who originally reported the breach / suspected breach	
Date and time the breach / suspected breach was reported	
Who was the breach / suspected breach reported to?	
Has the Data Protection Officer been informed?	
Has the Data Breach Response Team been notified?	
What are the details of the breach / suspected breach (include as much detail as possible) **NB: An investigation must be undertaken where appropriate**	
Who is responsible for the breach i.e. the school as data controller, a joint data controller or a data processor?	
Is the breach ongoing or has it been contained? What steps have been taken to minimise the effects of the breach?	

Information	Response
Is any other information required in order to assess the extent of the breach / the risk to data subjects? If so, specify that information here.	
Whose data has / may have been compromised as a result of the breach / suspected breach?	
Type of data involved in the breach / suspected breach	
Does the breach / potential breach involve Special Category Personal Data or information about criminal offences?	
What is the likely risk to individuals?	
Is there likely to be a high risk to individuals?	
Does the breach need to be reported to the ICO? **If yes, and if the breach happened more than 72 hours ago, what is the reason for the delay if notifying the ICO?**	
If the breach has already been reported to the ICO, confirm the date and time the report was made, who made the report and whether the report was made within 72 hours	
If a report has been made to the ICO, what advice or recommended actions have been given? **Specify any sanctions that are issued by the ICO following a breach.**	
If a report to the ICO is not being made, confirm the reasons why and whether the decision needs to be kept under review	

Information	Response
Do the data subjects affected need to be notified about the breach? If so, confirm who will notify them and how and when they will be notified. **If data subjects are not going to be informed, explain the reasons why.**	
Does the breach need to be reported to the Police?	
Do any other steps need to be taken e.g. comms to stakeholders, provision of complaints policy, consult legal advisors, notify insurers, external IT support.	
Is there likely to be press / media interest as a result of the breach? If so, have the appropriate protocols for handling media enquires been followed?	
Outline the actions that need to be taken in response to the breach / suspected breach to reduce the risk of a re-occurrence and who is responsible for implementing them and the relevant timescales. This should include whether an investigation under the school's disciplinary policy is recommended. **NB: The information provided in response to this question is likely to be a summary as a more detailed report / audit is likely to be required following a data breach which is notified to the ICO.**	

Appendix 2 – Contact details

ICO - 0303 123 1113

HR Support – HfL Education Limited (hrservices@hfleducation.org)

IT Support – Interm IT Limited (richard.spragg@intermit.co.uk)

Legal Support – Brown Jacobson (Vicki.Hair@brownejacobson.com)

Insurers - Risk Protection Arrangement (RPA.CM@davies-group.com)

Appendix 3 – Glossary of Terms

Biometric Data	Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics which allow or confirm the unique identification of that person, such as fingerprints.
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the Processing of Personal Data relating to them.
Data Controller	Exercises overall control over the purposes and means of the Processing of personal data.
Data Processor	Acts on behalf of, and only on the instructions of, the relevant Controller.
Data Protection Officer (DPO)	Monitors internal compliance of an organisation, informs and advises on data protection obligations.
Data Subject	Data Subjects for the purpose of this policy include all living individuals about whom we hold Personal Data.
Data User	Data Users include employees, volunteers, governors whose work involves using Personal Data.
Information Commissioner's Office (ICO)	Independent public body responsible for ensuring compliance with the UK's data protection regulations by providing guidance, investigating breaches of the regulations and dealing with complaints.
Parent	Parent has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child
Personal Data	Any information relating to an identified or identifiable natural person, which could be as simple as a name or a number, or which could include other identifiers e.g. date of birth, photo, IP address etc.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.
Privacy by Design	Implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR
Processing	Any operation which is performed on Personal Data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, erasure or destruction.
Special Category Data	Personal Data revealing or concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), health and sexual orientation.
Subject Access Request (SAR)	A formal request from a data subject for information, including Personal Data, which an organisation holds about them.