Data Breach Response Plan

June 2025

……. ……

Headteacher **Date**

Review Date: June 2027

1. **Introduction**

1.1 Knightsfield School (The School) has implemented appropriate technical and organisations measures to avoid data security breaches. However, in the event that a data security breach happens, we recognise that is important that the Trust is 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 data breach, the Trust is also required to notify the individuals affected by the breach. However, in the interests of transparency, the Trust recognise 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 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.

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.

1.8 The School's Data Protection Officer (DPO) is Lucy Pope. Any questions or concerns about the operation of this plan should be referred in the first instance to the DPO. Please email lpope@knightsfield.herts.sch.uk

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 Breaches can be categorised according to the following three well-known information security principles:

2.3.1 "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data;

2.3.2 "Integrity breach" - where there is an unauthorised or accidental alteration of personal data;

2.3.3 "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

2.4 Depending on the circumstances, a breach can relate to the confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

2.5 A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

2.6 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 School Data Breach Log set out in Appendix 1 so that we keep records of all such incidents. However, depending on the circumstances of the breach, it may or may not require notification's to the ICO and communication to affected individuals.

2.7 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 is 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 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 School 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 the Trust who becomes aware of a suspected or actual data security breach must inform the DPO by email without delay. The email address for contacting the lpope@knightsfield.herts.sch.uk and the email account should be regularly reviewed by the DPO. The Headteacher should also be copied into the email.

5.2 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.

5.3 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:

5.3.1 establish if a breach has happened;

5.3.2 establish the nature and cause of the breach;

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

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

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

5.4 The DPO should contact member of staff who made the report if further information is required.

5.5 During the course of their investigation, the DPO should consider whether to involve the Data Breach Response Team which consists of:

5.5.1 The Headteacher

5.5.2 Con-Ed IT support

5.6 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 Headteacher must fulfil the responsibilities of the DPO set out in this Data Breach Response Plan.

5.7 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.

5.8 The DPO should consider whether input is required from the School's IT or HR support team (as provided by Con-Ed for IT and Herts for Learning for HR) 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.

5.9 Depending on the circumstances, the DPO should also consider whether a notification of a potential Professional Indemnity Claim needs to made under the Risk Protection Arrangement, whether legal advice is required and if the incident needs to be reported to the Police and the Local Authority. The DPO should also consider if specialist IT support is required in order to contain and manage a breach.

5.10 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.

5.11 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.

5.12 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:

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

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

5.12.3 the likely consequences of the personal data breach;

5.12.4 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.

5.13 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 School does not yet have all the required information and if further details will be provided later on.

5.14 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.

5.15 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.

5.16 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 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:

5.16.1 description of the nature of the breach;

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

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

5.16.4 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.

5.17 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.

5.18 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.

5.19 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.

5.20 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.

5.21 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.

5.22 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.

5.23 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's 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.

5.24 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.

5.25 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 Knightsfield School 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 School is closed 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 An 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 Headteacher 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 they 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 school is closed due to the school holidays and, depending on the circumstances, advice should be sought from the ICO on the steps the Trust 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 and authorised at least every two years by the Headteacher.

Appendix 1 – Data Breach Log for Knightsfield School

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 Trustl'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.

DATA BREACH REPORT

Date Breach Identified:		**Title:**	
Time:		**Breach Ref No:**	
Summary of the Breach:			
How was the breach identified:			
Immediate Remedial Action Taken:			
Investigation:			
Risk Assessment: Low/ Med/ High (Assess the risk to the rights and freedoms of the affected individual)		**Justification:**	
Factors considered in Risk Assessment: **The type of breach:**			

The nature, sensitivity, and volume of personal data: **The ease of identification of individuals:** **The severity of consequences for individuals:** **The special characteristics of the individual:** **The special characteristics of the data controller**[1]: **The number of affected individuals:**		
Report to the Data Subject [2]		
Report to the ICO [3]		
Additional Action Required: •		
Reviewed by Data Protection Officer	**Signed**	
	Name (Printed)	
	Date	

Reviewed by Headteacher	**Signed**	
	Name (Printed)	
	Date	

Notes:[1] **Trusted***:* The Text below is an extract from a guidance document "GDPR Data Breach Example Scenarios June 21", which is provided as part of the GDPR Toolkit (Herts for Learning)

> *The following is taken from a document issued by the EU prior to GDPR being introduced. However, the content would still appear to be valid, and may help when deciding the risks involved when data is accidentally sent or shared with the incorrect recipients:*
>
> *"Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach, whereby personal data is disclosed to a third party or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered "trusted". In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals."*

[2] From the ICO's guidance: **When do we need to tell individuals about a breach?**

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the UK GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

[3] From the ICO's guidance: **What breaches do we need to notify the ICO about?**

When a personal data breach has occurred, you need to establish the likelihood of the risk to people's rights and freedoms. If a risk is likely, you must notify the ICO; if a risk is unlikely, you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.