Data Protection Policy and Data Breach Response Plan

This is an internal policy which works alongside school GDPR logs and procedures (see main GDPR folder). It is to be read in conjunction with the school Privacy Notice (website) and Privacy Notice for Staff, Governors and Volunteers (internal policy). The Herts Online Safety Policy is followed by the school to ensure all stakeholders, including staff, pupils and parents are abiding by the acceptable use standards.

Introduction

1.1 Four Swannes Primary School has implemented appropriate technical and organisational policies, procedures and measures to avoid data security breaches. However, in the event that a data security breach happens, we recognise that is important that the School 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 General Data Protection Regulation ('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 school GDPR policy and procedure.

1.3 The procedures set out in this document are particularly important as, prior to the GDPR, there was no obligation on the School to notify the Information Commissioner's Office ('ICO') of data security breaches, although it was good practice to report serious breaches.

1.4 The GDPR requires the School 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, which is a subjective measure determined jointly by the Data Breach Response Team (see 5.7). In the event that a report is not made within 72 hours, the School is required to provide the reasons for the delay in reporting it to the ICO.

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

1.6 If the School 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 policy is to ensure that we protect the Personal Data of our stakeholders and minimise any risks to them following a breach.

1.7 The School will ensure that staff are trained to recognise and report personal data breaches. Refresher training must be provided at least every two years.

1.8 We rely on our staff to be alert to the risk of data security breaches and to follow the procedures set out in this policy 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 School uses School Consulting Ltd, an external DPO service.

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’s Data Breach Log (within the electronic GDPR folder). However, depending on the circumstances of the breach, it may or may not require notification 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 (and school-based Deputy DPO) will 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 School 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 School 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 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 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

Step-by-Step Response Plan (for all staff):
1. Immediately report any suspected or actual breach to the Headteacher, Deputy DPO, or via

the dpo@ email.
2. Do not attempt to investigate or resolve independently – await instruction.
3. The Deputy DPO will assess and record details in the Breach Log.
4. If in doubt, the external DPO will be consulted, particularly if ICO reporting may be required.
5. Contain the breach where possible (e.g. secure documents, isolate IT systems) following Deputy DPO instructions.
6. Cooperate fully with any investigation or requests for information.
7. Do not contact data subjects directly unless authorised by the Headteacher/Deputy DPO.

5.1 A member of staff within the school, who becomes aware of a suspected or actual data security breach, must inform the Headteacher, the Deputy DPO (Office Manager), or the DPO of the School by email without delay. The email address for contacting the DPO is dpo@fourswannes.herts.sch.uk and the email account is regularly reviewed by the Deputy DPO internally. The DPO is contacted by the above party/parties as required.

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 The Deputy DPO, will then be responsible for assessing whether the breach or suspected breach needs to be formally escalated to the DPO. If the Deputy DPO decides not to escalate it to the DPO, the Data Breach Log 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 is reviewed by the DPO termly during DPO Inspection Visits. The external DPO must always be informed if there is any doubt whether this would reach the threshold of reporting to the ICO.

5.4 If the Deputy DPO decides to escalate a breach or suspected breach to the DPO, they must do so without delay. Where possible, the Data Breach Log must be completed with as much information as possible. 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 or over the phone in extreme cases, though a written record is required.

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

5.5.1 establish if a breach has happened;

5.5.2 establish the nature and cause of the breach;

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

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

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

5.6 The DPO will contact the Headteacher 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.

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

5.7.1 Headteacher and DPO as required, plus other staff at the Headteacher's request.

5.7.2 School Business Manager,

5.7.3 If the DPO is unavailable for any reason, Deputy DPO must fulfil the responsibilities of the DPO set out in this Data Breach Response Plan. The Headteacher must have access to the email account identified above to which data breaches are reported.

5.8 If the Deputy DPO decides to involve the Data Breach Response Team, the above individuals will be copied into email correspondence and provided with regular updates on the investigation and response to the incident.

5.9 The Deputy DPO should consider whether input is required from the School IT or 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. Contact details for IT support are available in the office and the company used for the support is identified in the Supplier Compliance Log.

5.10 Depending on the circumstances, the Headteacher should consider whether the School's insurers should be notified in accordance with policy terms, whether legal advice is required and if the incident needs to be reported to the Police and the Local Authority. The Deputy DPO will also consider if specialist IT support is required in order to contain and manage a breach and whether the county Press Office 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.

5.11 If the breach or suspected breach has occurred at one of our Data Processors, the Deputy 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 School's responsibility along with guidance from the DPO, to decide whether to report any such breach to the ICO within 72 hours. Data Processor breaches must always be escalated to the external DPO, as the school retains legal responsibility.

5.12 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.

5.13 Depending on the timescales as to when a member of staff originally became aware of a breach, the Deputy 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 School has fully investigated or contained the breach. A report to the ICO must contain the following information:

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

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

5.13.3 the likely consequences of the personal data breach;

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

5.14 The DPO or Deputy 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 or Deputy 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.

5.15 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.

5.16 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.

5.17 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 Deputy DPO must liaise with the Headteacher in relation to how the issue should be communicated to the relevant stakeholders. The school should 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: All external communications (letters to parents, media responses) must be cleared by the Headteacher and Deputy DPO before issue, and the external DPO may provide wording or review if requested.

5.17.1 description of the nature of the breach;

5.17.2 the name and contact details of the Deputy DPO or other contact point;

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

5.17.4 a description of the measures taken or proposed to be taken by the School 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, the above information may need to be given to parents / carers for affected pupils who are aged 13 or under.

5.18 If the Deputy DPO/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 School 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.

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

5.20 In certain circumstances, where justified, and on the advice of law-enforcement authorities, the School 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.

5.21 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.

5.22 In the event that the DPO concludes that it is not necessary to refer the breach to the ICO, the Deputy DPO must still complete the Data Breach Log and clearly set out the reasons why the DPO or Deputy DPO is satisfied that a referral is not required. The school must keep the decision under review and prepare 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.

5.23 Once the breach has been contained and action taken to stop or mitigate the breach, the Deputy DPO or 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.

5.24 As part of the review process, the school 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 School 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.

5.25 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.

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

5.27 Record Keeping

5.27.1 Record Keeping logs will be kept for a period of 6 years from the date of the incident. This aligns with the school's data retention schedule.

5.27.2 The Data Protection Officer checks processes and controls at least annually and logs of Data Risk, Data Breaches, Subject Access Requests are maintained by the school and subject to inspection and interrogation during DPO visits.

6. School holidays

6.1 The 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 and have 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 Deputy DPO will have the contact details for the Headteacher and IT support so that action can be taken without delay should a breach occur.

6.1.3 The Deputy 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 school is closed and has limited staff available due to the school holidays and, depending on the circumstances, advice should be sought from the ICO on the steps the School 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.

8. How do we protect our data?

8.1 Our data backup and security measures are documented in the Supplier Compliance Evidence folder; part of the GDPR folder within the school central electronic filing system, accessible by senior and key support staff. This organisation, (details in section 9) responsible for data backup has detailed the current security measures and storage processes/methods. Any changes to this system or procedure will be evident by an updated version number of that document.

9. Contact for IT Support

The Deputy DPO must maintain up-to-date contact details for IT support, insurers, and legal advisors.

HFL Andy Lees 01438844777

itsupport@hfleducation.org

10. Contact the Shared Anti-Fraud Service if necessary (SAFS)

a. 0300 123 4033
b. fraud.team@hertfordshire.gov.uk
c. www.hertfordshire.gov.uk/fraud