Data Protection Policy and Data Breach Response Plan

GEORGE STREET PRIMARY SCHOOL

"Believing in Every Child"

Approved by: **Head Teacher:** Angela Hughes
Last reviewed on: **14th July 2026**
Next review due by: **Summer term 2028**

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 followed by the school to ensure all stakeholders, including staff, pupils and parents are abiding by the acceptable use standards.

Introduction

1.1 George Street 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 our Data Protection Policy and Data Security Policy

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 We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, the local authority or other background check agencies. We may perform online searches as part of the recruitment process, due to guidance in Keeping Children Safe in Education (KCSIE). To comply with the General Data Protection Regulations, we will inform you if you have a choice in this.

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 aware of and are trained on GDPR and data security at least biennially.

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

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 (detailed in the Data Breach Log), or the DPO of the School by email without delay. The email address for contacting the DPO is dpo@georgestreet.herts.sch.uk and the email account is regularly reviewed by the Deputy DPO and the Headteacher. The DPO is contacted by the above party/parties as required. The Deputy DPO is the School Business Manager.

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.

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,

5.7.2 Office Manager/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.

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:

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 will need to be given to parents / carers for affected pupils 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.

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

Herts for Learning IT Services, **ITsupport@hertsforlearningeducation.org**, phone number **01438 844777**

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

Appendix A

Data Protection Complaints and Information Rights Procedure (including Subject Access Requests)

1. Purpose

The school takes data protection concerns seriously and will consider complaints about the way personal data has been handled.

This procedure explains how the school will manage data protection complaints and concerns, including concerns linked to subject access requests, other information rights requests, personal data handling, retention, accuracy, security and alleged data breaches.

This procedure applies to both primary and secondary schools and should be read alongside the school's Data Protection Policy, Privacy Notice, Subject Access Request process, Data Breach Response Procedure and wider complaints arrangements.

2. What this procedure covers

This procedure covers concerns about the way the school has handled personal data or responded to an information rights request, including a subject access request.

It may include concerns about whether the school has followed the correct process, responded within the relevant statutory timescale, or whether specific personal data has been missed, incorrectly disclosed, wrongly withheld or handled in a way that raises a genuine data protection concern.

This procedure is not intended to reopen wider school complaints, safeguarding concerns, behaviour matters, SEND issues, admissions, exclusions, HR matters, parental disputes or disagreements with school decisions simply because personal data is mentioned within those matters. Where a concern is mainly about another school process, the school will decide the appropriate route for dealing with it. A concern will not automatically become a data protection complaint simply because personal data is referred to within a wider school matter.

3. How to raise a data protection complaint

Data protection complaints should be made in writing where possible and sent to:

Portia Ward, School Business Manager, sbm@georgestreet.herts.sch.uk

Complaints and information rights requests should be sent to the school through this contact route, not directly to the school's External Data Protection Officer. This ensures the school, as Data Controller, can log the matter, check identity where needed and manage statutory timescales.

The complaint should explain:

- what the concern is
- whose personal data is involved
- what request, incident or decision the complaint relates to
- what outcome is being sought

- any specific information the person believes has been missed, mishandled or wrongly disclosed

The school may ask for clarification where the concern is unclear, where further information is needed, or where the complaint includes broad or general allegations that cannot reasonably be investigated without more detail.

4. Complaints linked to ongoing Subject Access Requests or information rights requests

Where a subject access request or other information rights request is already being processed, the school will normally complete that process before considering a complaint about the outcome.

This is because the school cannot fairly assess whether information has been missed, withheld or handled incorrectly until the response has been completed and the requester has had the opportunity to review it.

The school may still consider a genuine procedural concern during an ongoing request where appropriate, for example if the requester believes the school has failed to acknowledge the request, has asked for unnecessary identification, or has refused to process the request. However, complaints about the scope of searches, redactions, exemptions, missing information or dissatisfaction with the eventual disclosure will normally be considered after the response has been issued.

The school will not normally enter into repeated correspondence or debate while a Subject Access Request is still being processed. Relevant correspondence may be acknowledged and considered as part of the ongoing process where appropriate.

5. Clarification, changes and additional requests

Requesters may clarify the scope of a Subject Access Request where this is genuinely needed.

However, repeated changes, new requests, additional search terms, new date ranges, additional named individuals, further systems, or additional categories of information may be treated as a new request. Where clarification is required, the statutory timescale may be paused until clarification is received.

If the requester significantly expands the request after it has already been logged and searches have begun, the school may decide whether the new points can reasonably be included within the existing request or whether they should be dealt with separately.

Where the same requester submits more than one request relating to the same person, the same records, the same incident, or substantially the same information, the school may manage those requests together where it is reasonable to do so. The school will not normally duplicate searches or run parallel request processes for the same data, as this would be disproportionate and could create confusion or unnecessary delay.

If a further request is received while an existing request for the same or substantially similar information is still being processed, the school may confirm that the further request will be considered as part of the existing request where appropriate. Alternatively, the school may treat it as a separate request with its own timescale if it raises genuinely new issues or seeks different information.

The school will take a reasonable and proportionate approach, but requesters should not expect a live request to be repeatedly reworked, duplicated or restarted each time further correspondence is sent.

6. Extensions to the response period

Where a request is complex, or where the requester has made a number of requests, the school may extend the response period by up to a further two months, in line with UK GDPR.

The school will inform the requester within the initial one-month period where an extension is being applied and will explain the reason for this.

The decision to apply an extension is made by the school, based on the complexity, volume and circumstances of the request. Requesters do not need to agree to the extension for it to apply. Where the school has notified the requester within the initial one-month period and explained why an extension is needed, the extended statutory timescale will apply. The use of a lawful extension is part of the subject access process and does not mean that the school has failed to comply with the request.

7. Fees for Subject Access Requests

The school will not usually charge a fee for responding to a Subject Access Request.

A request will not be charged for simply because it is complex, time-consuming or involves a large amount of information. Where a request is complex, or where a requester has made a number of requests, the school may consider whether an extension to the response period is appropriate.

The school may only consider charging a reasonable fee where this is permitted by data protection law, for example where a request is manifestly unfounded or excessive, or where the requester asks for further copies of information already provided. Any decision to charge a fee must be considered carefully and documented before the requester is informed.

8. Searches carried out by the school

The school is responsible for deciding what searches are reasonable and proportionate.

In doing so, the school may take into account:

- the wording and scope of the request
- the information likely to be held
- the systems used by the school
- the age and location of the information
- the burden of searching
- whether the search is likely to produce relevant personal data
- the rights and freedoms of other individuals
- safeguarding, confidentiality and legal considerations

Requesters may suggest where they believe relevant information may be held. However, they cannot require the school to search every system, device, email account, staff member, archive or historic record unless this is reasonable and proportionate in the circumstances.

The school will not carry out broad, speculative or repeated searches where it has already taken reasonable steps to locate the personal data falling within the scope of the request.

9. Redactions, exemptions and third-party information

The school may withhold or redact information where required or permitted by law.

This may include information that relates to other children, parents/carers, staff, safeguarding concerns, confidential records, legal advice, management information, ongoing investigations, or information that would adversely affect the rights and freedoms of another person.

The school will consider exemptions and redactions on a case-by-case basis. The fact that information relates to the requester, or mentions the requester, does not automatically mean it can be disclosed in full.

In school settings, records may often contain mixed information about several people. This is particularly common in safeguarding records, behaviour records, complaints records, CPOMS-style records, emails and staff notes. The school must balance the requester's rights with the rights, safety and confidentiality of others.

Where information has been lawfully withheld or redacted, the school is not required to release it simply because the requester disagrees with the decision or raises a complaint. A complaint or challenge may lead the school to review a specific redaction or withholding decision, but it will not automatically result in the information being disclosed.

Where the school reviews a decision and remains satisfied that the original reason for withholding or redacting the information is sound, the school may confirm that the original decision stands.

10. Use of external advice, template letters or AI-generated correspondence

The school recognises that individuals may seek advice or use template letters, online tools or AI-generated wording when raising data protection concerns or making information rights requests. The school will consider the substance of the correspondence, rather than the form in which it is drafted.

However, correspondence must still be clear, specific and manageable. The use of lengthy, repetitive or generic wording will not require the school to expand the request beyond what has reasonably been asked for, repeat searches already completed, or respond separately to every legal assertion where the school has already addressed the substance of the matter.

Where correspondence introduces new issues, new time periods, new search terms, additional individuals or further categories of information, the school may treat those points as a new request or may ask the requester to clarify what they are asking for.

The school is responsible for deciding how to process a Subject Access Request lawfully and proportionately. Requesters may identify specific information they believe the school holds, but they cannot require the school to adopt a particular search method, search every possible location, disclose exempt information, or disregard the rights and freedoms of other individuals.

Where a requester repeatedly sends further correspondence before the school has completed its response, the school may acknowledge the correspondence and confirm that it will be considered as part of the ongoing process where relevant. The school will not normally provide repeated interim responses or enter into ongoing debate while the request is still being processed.

11. Complaints after a response has been issued

If, after receiving the school's response, the requester believes that specific personal data has been missed or that the request has not been handled correctly, they should explain clearly what they believe is missing or incorrect.

Data protection complaints must be reasonable, specific and capable of being considered by the school. Where a requester believes that a Subject Access Request or other information rights request has not been handled correctly, they should identify the specific information, document, search area, redaction or decision they are concerned about.

A complaint should not simply ask the school to repeat the whole process, carry out all searches again, reconsider every redaction, or provide a different outcome without explaining what specific issue needs to be reviewed.

The school will consider specific and reasonable concerns. However, general dissatisfaction, disagreement with lawful redactions, or a belief that more information must exist will not automatically require the school to repeat searches, reopen the request or re-run the process.

Where the school is satisfied that reasonable searches have already been carried out and the response has been properly handled, it may confirm that no further action will be taken.

12. Timescale for responding to data protection complaints

The school will respond to data protection complaints without undue delay and will aim to provide a response within one calendar month.

Where a matter is complex, where further enquiries are needed, or where the complaint overlaps with another school process, the school may require additional time. The school will keep the complainant informed where this is the case.

13. Repeated, excessive or unreasonable correspondence

The school will always consider genuine data protection concerns.

However, the school is not required to respond repeatedly to the same point where it has already provided a clear response. The school may manage repeated, excessive or unreasonable correspondence in line with its usual complaints or communications procedures.

Where correspondence becomes unreasonable in volume, frequency or tone, the school may set appropriate communication boundaries while still ensuring that any valid information rights request is handled in line with data protection law.

14. Role of the External Data Protection Officer

The school has an internal contact route for data protection matters, normally through its DPO@ email address, where used, or other nominated internal Data Protection Lead.

The External Data Protection Officer provides advice and support to the school. The External DPO is not the school's complaint handler and does not correspond directly with parents, pupils, staff, requesters or complainants.

Where a parent, pupil, requester or complainant contacts the External DPO directly, the External DPO may redirect them to the school's nominated contact route. Where appropriate, the External DPO may alert the school that direct contact has been received, but the individual

should still be directed to the school's own contact route so the matter can be logged and handled by the school.

The school may seek advice from its External Data Protection Officer when handling data protection complaints, Subject Access Requests or other information rights requests.

The External DPO may advise the school on legal requirements, proportionality, timescales, searches, redactions, exemptions and complaint handling. The school remains responsible for managing correspondence and for decisions about its own records and responses.

15. Information Commissioner's Office

Individuals have the right to raise concerns with the Information Commissioner's Office.

The ICO will usually expect individuals to have raised the matter with the school first and allowed the school a reasonable opportunity to respond.

The ICO can be contacted via its website: www.ico.org.uk

16. Review

This procedure should be reviewed periodically and updated where there are changes to data protection law, ICO guidance or the school's internal processes.