



Data Protection Policy

1. Monitoring and Review

The DPO is responsible for monitoring and reviewing this policy.

This policy will be updated if any other changes are made to relevant legislation, as implemented, that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every year and shared with the full Governing Body.

Created: May 2018

Revised: March 2023

Ratified by the Governing Body: May 2018

Date of Last Review: March 2024

Date of Next Review: Spring 2025

Change History	Date	Change(s) Made	Change Author	EDI ¹
V2.4	Mar 2024	Policy reviewed - no changes	RBO	Yes
V2.3	Mar 2023	Sections 7.1, 8, 9.1, 9.3, 9.4, 11, 12, 13, and 15 were updated, and 7.2 removed to reflect the changes to the UK GDPR. Appendix 1 was updated. The policy is based on the model policy from The Key for School Leaders.	RBO	Yes
V2.2	Mar 2022	The policy was reviewed and updated to reflect the UK's departure from the European Union, and the legislation changed as a result.	RBO	Yes
V2.1		Policy reviewed - referenced the Data Protection (Independent Complaint) Bill 2019	RBO	
V2.0		Policy based on The Key for School Leaders model Data Protection policy created.	RBO	

2. Aims

2.1 The Reach Free School aims to ensure that all personal data collected about staff, pupils, parents, guardians and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

3. Legislation and guidance

3.1 This policy meets the requirements of the:

3.2 UK General Data Protection Regulation (UK GDPR) - the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#).

3.3 [Data Protection Act 2018 \(DPA 2018\)](#)

3.4 This policy is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#).

3.5 This policy meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.

¹ Any changes or revisions to the policy have considered equality, diversity and inclusion.

3.6 This policy also reflects the ICO's [guidance](#) for the use of surveillance cameras and personal information.

3.7 This policy also complies with our funding agreement and articles of association.

4. Definitions

Term	Definition
Personal data	<p>Any information relating to an identifiable individual. This may include the individual's:</p> <ul style="list-style-type: none"> ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns) where used for identification purposes ● Health – physical or mental ● Sex life or sexual orientation
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.</p>
Data subject	<p>The identified or identifiable individual whose personal data is held or processed.</p>
Data controller	<p>A person or organisation that determines the purposes and the means of processing personal data.</p>
Data processor	<p>A person or body other than an employee of the data controller who processes personal data on behalf of the data controller.</p>
Personal data breach	<p>A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.</p>

5. The Data Controller

5.1 The Reach Free School processes personal data relating to parents, guardians and carers, pupils, staff, Governors, visitors and others, and therefore is a Data Controller.

5.2 The School is registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required.

6. Roles and responsibilities

6.1 This policy applies to **all staff** employed by the School, the Governing Body, and external organisations or individuals working on our behalf. Staff and Governors who do not comply with this policy may face disciplinary action.

6.2 The Governing Body

The Governing Body is responsible for ensuring that our School complies with all relevant data protection obligations.

6.3 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of their activities directly to the Governing Body and, where relevant, report their advice and recommendations on school data protection issues to that Body.

The DPO is also the first point of contact for individuals whose data the school processes and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

The Reach Free School's DPO is Debra Pash, who is contactable via email at dpo@reachfree.co.uk.

6.4 Headteacher

The Headteacher is the Data Controller's representative on a day-to-day basis.

6.5 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the School of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties

7. Data Protection Principles

7.1 The UK GDPR is based on data protection principles that The Reach Free School must comply with.

7.2 The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the School aims to comply with these principles.

8. Collecting personal data

8.1 Lawfulness, fairness and transparency

The Reach Free School will only process personal data where there are one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual, e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the School or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent, guardian or carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to maintain confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to maintain confidentiality under law

- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent, guardians or carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use it in ways that have unjustified adverse effects on them.

8.2 Limitation, minimisation and accuracy

The Reach Free School will only collect personal data for specified, explicit and legitimate reasons. When we first collect their data, we will explain these reasons to the individuals.

If the School wants to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where necessary to do their jobs.

When staff no longer need their personal data, they must ensure it is deleted or anonymised. This will be done in accordance with the school's records management policy.

9. Sharing personal data

The School will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent, guardian or carer that puts the safety of our staff at risk
- The School needs to liaise with other agencies – we will seek consent as necessary before doing this
- Suppliers or contractors need data to enable us to provide services to staff and pupils – for example, IT companies. When doing this, the school will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

The School will also share personal data with law enforcement and government bodies where we are legally required to do so.

The School may also share personal data with emergency services and local authorities to help them respond to an emergency that affects our pupils or staff.

Where the School transfers personal data to a country or territory outside the UK, it will do so in accordance with data protection law.

10. Subject access requests and other rights of individuals

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to see the personal information that the School holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this is not possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to complain to the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

10.2 Children and subject access requests

Personal data about a child belongs to that child, not the child's parents, guardians or carers. For a parent, guardian or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children under 12 are generally not regarded as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents, guardians or carers of pupils under 12 at The Reach Free School may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded as being mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents, guardians or carers of pupils aged 12 and above at The Reach Free School may not

be granted without the express permission of the pupil. This is not a rule, and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

10.3 Responding to Subject Access Requests

When responding to requests, the School:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual the School will comply within three months of receipt of the request, where a request is complex or numerous. The School will inform the individual of this within one month and explain why the extension is necessary

The School will not disclose the information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we cannot reasonably anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, the School may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. We will consider whether the request is repetitive in nature when making this decision.

When the School refuses a request, it will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

10.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict the processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11. Parental requests to see the educational record

Parents or those with parental responsibility do not have a legal right to free access to their child's educational record from The Reach Free School. However, a certain amount of information is made available through the School's management information system, Arbor. Where other records are held, the School will endeavour to comply with requests to see this information. Requests for information should be addressed to the Data Protection Officer. The School will respond within one month. In certain situations, there may be a charge for this information.

12. Biometric recognition systems

Where the School uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use biometric prints to receive school dinners instead of paying with cash), we will comply with the [Protection of Freedoms Act 2012](#) requirements.

Parents, guardians and carers will be notified that the School uses a biometric recognition system via the Pupil Registration Form. The School will get written consent from at least one parent, guardian or carer before we take any biometric data from their child and first process it.

Parents, guardians or carers and pupils have the right to choose not to use the School's biometric system. The School will provide an alternative means of accessing the services for those pupils. For example, pupils can pay for school dinners using a pin code, if they wish.

Parents, guardians or carers and pupils can object to participation in the School's biometric recognition system, or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s), guardians(s) or carer(s).

Where staff members or other adults use the School's biometric system, we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any data already captured.

13. CCTV

The Reach Free School uses CCTV in various locations around the school site to ensure it remains safe. We will follow the [ICO's guidance](#) for the use of CCTV, and comply with data protection principles.

The School does not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO.

14. Photographs and videos

As part of our School's activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents, guardians and carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent, guardian or carer and pupil. Where we do not need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Data protection legislation does not cover any photographs and videos taken by parents, guardians or carers at school events for their own personal use. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons unless all the relevant parents, guardians or carers (or pupils, where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within School on notice boards and in School newsletters, the prospectus, etc.
- Outside School by external agencies such as the School photographer or newspapers, campaigns
- Online on our School website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with full personal information about the child, to ensure they cannot be identified.

See our 'Consent for Use of Photographs' form for more information on our use of photographs and videos.

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data impact assessments where the School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

16. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least eight characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for School-owned equipment (see our Online Safety Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

17. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

The School will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the School website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

19. Training

All staff and Governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the School's processes make it necessary.

20. Links with Other Policies

This data protection policy is linked to our:

- Freedom of Information Policy
- Online Safety Policy
- Child Protection Policy
- Pupil Registration Form
- Consent for the Use of Photographs Form

Appendix 1: Personal Data Breach Procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- The DPO will alert the Headteacher and the Chair of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure.)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#)
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identity theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page](#) of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
 - A description, in clear and plain language, of the nature of the personal data breach
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Date and time of the breach, and date and time of discovery
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be on the school's storage system
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and headteacher will share a report with the Governing Body termly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the Deputy Headteacher to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Other types of data protection breaches could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families