Sutton Valence Primary School

Data Protection Policy

Approved by:	Matthew Jones	**Date**: Sept 26
Last reviewed on:	Sept 26	
Next review due by:	Sept 27	
Approved by DPO:	Sept 2026	
Approved by Governors:	Sept 2026	

Contents

1. Aims 3

Get the knowledge you need to act at thekeysupport.com
© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

2. Legislation and guidance 3
3. Definitions 4
4. The data controller 5
5. Roles and responsibilities 5
6. Data protection principles 6
7. Collecting personal data 7
8. Sharing personal data 8
9. Subject access requests and other rights of individuals 8
10. Parental requests to see the educational record 10
11. CCTV 11
12. Photographs and videos 11
13. Artificial intelligence (AI) 12
14. Data protection by design and default 12
15. Data security and storage of records 13
16. Disposal of records 13
17. Personal data breaches 14
18. Complaints 14
19. Training 14
20. Monitoring arrangements 14
21 Links with other policies 14
Appendix 1: Personal data breach procedure 16

1. Aims

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Our school aims to ensure that all personal data collected about staff, pupils, parents 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.

2. Legislation and guidance

This policy meets the requirements of the:

- 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
- Data Protection Act 2018
- Data (Use and Access) Act 2025

It is based on guidance and resources published by the Information Commissioner's Office (ICO) on the UK GDPR and a policy paper from the Department for Education (DfE) on Generative artificial intelligence in education.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record on request.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual, whether identified directly or indirectly. This may include the individual's: - Name (including initials) - Identification number - Location data - Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

TERM	DEFINITION
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: › 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	Any activity that involves the use of personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual, and also includes transmitting or transferring personal data to third parties.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data. The data controller is responsible for establishing practices and policies in line with the UK GDPR.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. A data processor acts only on the instructions of the controller and does not determine the purposes or means of the processing.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

Our school processes personal data relating to parents and carers, pupils, staff, governors, visitors and others. In carrying out these activities, the school acts as a data controller.

The school has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

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

5.1 Governing board

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer (DPO)

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.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

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.

Our DPO is HY Solicitors and is contactable via dpo@wearehy.com.

Please contact the DPO with any questions about the operation of this data protection policy or the UK GDPR, or if you have any concerns that this data protection policy is not being or has not been followed.

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 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:
    - If they have 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

6. Data protection principles

We adhere to the principles relating to processing of personal data set out in the UK GDPR, which requires personal data to be:

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);
- Collected for specified, explicit and legitimate purposes (purpose limitation);
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed (data minimisation);
- Accurate and, where necessary, kept up to date (accuracy);
- Kept for no longer than is necessary for the purposes for which it is processed (storage limitation);

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- Processed in a way that ensures it is appropriately secure (security, integrity and confidentiality);
- Not transferred to another country without appropriate safeguards in place (transfer limitation); and
- Handled in a way that respects the rights of data subjects and allows them to exercise those rights (data subject rights and requests)

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 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 or another person i.e. 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 or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) 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/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 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 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

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

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/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 personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want 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 it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

8. Sharing personal data

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

There will be certain circumstances where we may be required to share personal data. These include, but are not limited to, situations where:

- There is an issue with a pupil, or a parent or carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor 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

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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests (SARs)

By law, individuals have a right to make a 'subject access request' (SAR) to gain access to 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 isn't 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 lodge a complaint with 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 can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

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

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent 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 below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our 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.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary (these timeframes continue to apply when the school is closed during holidays)

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or 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 can't reasonably anonymise, and we don't 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, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we 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.

9.4 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
- Receive certain information about the data controller's processing activities
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that 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 personal 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.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it, however the fee must not exceed the cost of supply.

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

We use 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.

We do 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 prominent signs explaining that CCTV is in use.

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

12. Photographs and videos

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

We will obtain written consent from parents and carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parents/carers and the pupil.

Any photographs and videos taken by parents and carers at school events for their own personal use are not covered by data protection legislation. 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/carers have agreed to this.

Any photographs and videos taken by parents and carers at school events for their own personal use are not covered by data protection legislation. 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/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 brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, 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 any other personal information about the child, to ensure they cannot be identified.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Sutton Valence Primary School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Sutton Valence Primary School will treat this as a data breach and will follow the personal data breach procedure outlined in appendix 1.

14. 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 protection impact assessments (DPIAs) 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

15. 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 staffroom tables, 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 made up of 4 random, unrelated words, or that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- 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 / acceptable use agreement)
- 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)

16. 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.

17. 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 after becoming aware of it. 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

We will also notify the data subject where we are legally required to do so.

18. Complaints

We take any complaints about how we collect and use personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us at any time by contacting the headteacher or our DPO dpo@wearehy.com.

Upon receiving a complaint, we will:

- Acknowledge receipt of the complaint within 30 days of receiving it
- Without undue delay, take appropriate steps to respond to the complaint, including:
    - Making appropriate enquiries based on the circumstances of the complaint
    - Keeping the complainant informed on the progress of the investigation
- Without undue delay, inform the complainant of the outcome of the investigation

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.

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

20. Monitoring arrangements

The headteacher and DPO are responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy notices
- Online Safety Policy
- Acceptable Use Policy
- Child Protection Policy

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the school and the Data Protection Officer (DPO) by emailing dpo@wearehy.com
- The school will investigate the report, with advice from the DPO, to establish the circumstances of the incident and whether a personal data breach has occurred. This will include considering 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
- If a breach has occurred or it is considered to be likely that is the case, the school will ensure that the incident is appropriately escalated internally and that the DPO is provided with the information required to advise on the breach.
- The school will take appropriate steps to contain and minimise the impact of the breach. The DPO will advise the school on appropriate mitigative actions based on the nature and circumstances of the breach. The school should liaise with relevant staff, data processors, IT providers or other third parties where necessary to implement those actions.
- The DPO will advise the school on the level of risk presented by the breach, including the potential consequences for affected individuals and the likelihood of those consequences occurring, taking account of any steps taken or proposed to mitigate the risk.
- The DPO will advise the school on whether the thresholds for notification to the ICO under Article 33 UK GDPR and/or communication to affected individuals under Article 34 UK GDPR are met. The school, as data controller, remains responsible for determining and ensuring that its statutory notification obligations are complied with.
- The school will document the outcome of the breach assessment and any decisions taken, including whether the breach is reportable to the ICO and/or affected individuals. The DPO's advice should also be retained as part of the school's breach record.
- Where notification to the ICO is required, the school will ensure that the breach is reported without undue delay and, where feasible, within 72 hours of becoming aware of it. The DPO will advise and support the school in preparing the notification where required. The notification will include, where available:
    - 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

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- 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 required information is not yet known, the DPO will advise the school on the information that should initially be provided to the ICO and any subsequent information that should be provided as it becomes available.
- Where the school is required to communicate the breach to affected individuals, the DPO will advise the school on the content of the notification. The school will issue the notification to the affected individuals in clear and plain language, including:
    - 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 advise the school on whether it would be appropriate to notify any relevant third parties that may assist in mitigating the potential impact on affected individuals, such as the police, insurers, banks or credit card companies. The school will be responsible for making any such notifications.
- The school will document each personal data breach, irrespective of whether it is reported to the ICO. The DPO will provide advice on the information that should be recorded where required. :
    - 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 stored in a secure folder on the SharePoint.
- Following a breach, the school will review the circumstances of the incident and consider any measures required to reduce the risk of recurrence. The DPO will provide advice and recommendations where appropriate.
- The school will periodically review recorded data breaches to identify any trends or patterns requiring further action. The DPO may advise the school on any identified data protection risks and appropriate measures to address them.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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 advise the school to liaise with its ICT support provider to determine whether the email can be recalled from external recipients and removed from the school's email system, retaining a copy where required as evidence.
- Where an email recall is unsuccessful or cannot be confirmed as successful, the DPO will advise the school on whether it would be appropriate to contact the unauthorised recipient(s), explain that the information was sent in error, and request that the information is deleted and not shared, published, saved or replicated.

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- Where appropriate, the DPO may advise the school to seek written confirmation from the unauthorised recipient(s) that they have complied with any request to delete the information.
- Where there is a risk that the information may have been made publicly available, the DPO will advise the school on appropriate steps to establish whether this has occurred and, where necessary, to contact the relevant publisher, website owner or administrator to request its removal and deletion.
- Where safeguarding information is compromised, the DPO will advise the school to inform the designated safeguarding lead and, where appropriate, consider whether any of the school's local safeguarding partners should also be notified.

Non-anonymised pupil exam results or staff pay information being shared with governors

- Notify the Headteacher and Data Protection Officer (DPO) immediately.
- Ask recipients not to copy, download, forward or discuss the information.
- Securely recall or delete electronic files and collect or destroy printed copies, requesting confirmation where appropriate.
- Record what was shared, with whom, when and whether it was accessed or circulated further.
- The DPO will advise the school on the level of risk presented by the breach, taking into account the sensitivity of the information, the recipients' authorised roles and the potential impact on those affected.
- Record the incident and all actions taken in the school's data breach register.
- The DPO will advise the school on whether affected individuals are required to be informed where the breach is likely to result in a high risk to their rights and freedoms. .
- The DPO will advise the school on whether the breach is required to be reported to the ICO. Where notification is required, the school will ensure that this is done without undue delay and, where feasible, within 72 hours of becoming aware of the breach. .
- Investigate the cause and introduce preventive measures, such as anonymising or aggregating reports, restricting access and checking documents before circulation.
- Governors must maintain confidentiality and receive appropriate data protection training. Only the minimum personal information necessary for effective governance should be shared.

Hardcopy reports sent to the wrong pupils or families

- Notify the Headteacher and Data Protection Officer (DPO) immediately.
- Contact the unintended recipient and ask them not to read, copy or share the report.
- Arrange for the report to be securely returned or destroyed, with confirmation.
- Provide the correct report to the intended family using verified contact details.
- Record the incident, actions taken and information affected in the school's breach register.
- The DPO will advise the school on the level of risk presented by the breach, including whether sensitive, safeguarding, health or SEND information was disclosed.
- Inform the Designated Safeguarding Lead if safeguarding information is involved.
- The DPO will advise the school on whether the breach is required to be reported to the ICO and whether affected individuals are required to be informed. Where notification to the ICO is required, the school will ensure that this is done without undue delay and, where feasible, within 72 hours of becoming aware of the breach.
- Investigate the cause and introduce preventive measures, such as checking contact details, using a second-person check and improving report distribution procedures.
- Keep the matter confidential and share details only with those responsible for managing the incident.

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms