Data Protection Policy

Date	**June 2023**
Written by	**Hannah Doran**
Approved by	**Resources & Personnel Committee**
Approval date	**19/6/23**
Review date	**June 2024**

Contents

1. Introduction

Ivel Valley School and College is the Data Controller for all the Personal Data processed by the School. Everyone has rights with regard to how their personal information is handled. During the course of our activities we will process personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner.

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

2. Aims of this policy

The objectives of this Data Protection Policy are to ensure that Ivel Valley School and College and its governors and employees are informed about, and comply with, their obligations under the Data Protection

Act 2018 (DPA 2018), UK General Data Protection Regulation (UK GDPR) and with other Data Protection legislation.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. 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.
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	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.
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 of personal data.
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.
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, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with 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 Body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations. This responsibility is delegated to the Resources and Personnel Committee.

5.2 Data protection officer (external)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with, and advising on, data protection law.

Our DPO is HfL Education (formally Herts for Learning).

5.3 Data Protection Lead (in school)

The Business Manager and Network Manager are the Data Protection Leads at the school. They manage data protection on a day to day basis, including training, subject access requests, writing policies and procedures relating to data protection and investigating data breaches. They would also liaise with the DPO for advice and to report data breaches.

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

The Data Protection Leads are the first point of contact for individuals whose data the school processes, and for the ICO (who would also contact the DPO).

5.4 Headteacher

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

5.5 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 school's data protection leads 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

6. Data protection principles

The UK GDPR is based on data protection principles that our school must comply with.

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.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 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 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 one 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

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

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/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 which 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.

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

Individuals have a right to make a 'subject access request' 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:

- 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 Data Protection Leads.

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. 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
- Will acknowledge the request 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 unless the request is deemed manifestly unfounded or manifestly excessive (see below)
- 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

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 consider 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
- 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 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 Data Protection Leads. If staff receive such a request, they must immediately forward it to the Data Protection Leads.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free 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.

This right applies if 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. Biometric recognition systems

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

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can 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)/carer(s).

If staff members or other adults were to use the school's biometric system(s), 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 relevant data already captured.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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.

We have a separate CCTV Policy. Any enquiries about the CCTV system should be directed to the Data Protection Lead – hannah.doran@ivelvalley.beds.sch.uk

13. 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/carers and, where appropriate the pupils, 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 parent/carer and, if appropriate, the pupil.

We will obtain consent from staff to use their photographs and videos for any purpose other than for safeguarding or required for the education of the pupils.

Any photographs and videos taken by parents/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 magazines, brochures, newsletters, etc.
- For education records including Evidence for Learning
- For sharing with parents/carers e.g. on DoJo
- 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.

14. 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 Bard. We recognise 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.

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

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 protection 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
- 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.

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.

16.1 Data Protection and Use of IT Agreement

All staff are required to sign the Data Protection and Use of IT Agreement annually which covers:

- Clear desk/displays/hard copy data
- Workstation security
- Password security
- Security of portable equipment and devices
- Acceptable use
- Printing, copying and transmission of data
- Use of emails
- Data breaches

16.2 Network/server security

Security-related events should be reported to the IT team and to the DPO. Corrective measures will be prescribed as needed. Security-related events could include, but are not limited to, port-scan attacks and evidence of unauthorised access to privileged accounts.

IT infrastructure such as routers, switches, wireless access points etc. should be kept securely and only be handled by authorised personnel. They are:

- ICT Manager
- ICT Technician
- Headteachers
- Business Manager.

Backup Procedures (if required):

- Backup software must be scheduled to run routinely, as required, to capture all data as required.
- Backups should be monitored to make sure they are successful.
- A test restoration process will be run regularly.
- [If not using cloud backups] Backup media must be securely stored in a fireproof container.
- Backup media stored off-site must be transported and stored securely.

The school is currently covered by the government's Risk Protection Arrangement. This includes cyber cover but the school will only be covered when making a claim if we can evidence compliance with all of the conditions below:

- Have offline backups.
- Have completed NCSC Training for all Employees and Governors who have access to the Member's IT system by the 31 May 2022 or the start of the Membership Year, whichever is later.
- Register with Police CyberAlarm
- Have a cyber response plan in place.

[The following section will apply if servers are used – the school currently has no servers in use]

Servers should be physically located in an access-controlled environment. Unrestricted access to the computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment. Restricted access may be given to other staff or third-party support where there is a specific job function need for such access.

The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

Servers should have security software (Anti-Virus and Anti-Spyware) installed appropriate to the machine's specification.

Servers should always be password protected, and locked when not in use.

16.3 Access Control

Staff should only access systems for which they are authorised. Under the Computer Misuse Act 1990 it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation.

Formal procedures will be used to control access to systems. An appropriate manager must request each application for access and access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Staff with management responsibilities must ensure they advise IT or any other administrators of systems of any changes requiring such modification/removal.

Staff should pay particular attention to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals and documentation.

Any contractors (working on site or working remotely via a communications link) to maintain or support computing equipment and software must comply with the terms of this policy and any access control measures with which they are requested to comply with by school staff.

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. Disposal of redundant ICT equipment

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to: the Waste Electrical and Electronic Equipment Regulations 2018, the Data Protection Act 2018, the Electricity at Work Regulations 1989.

We will maintain a comprehensive inventory of all its ICT equipment including a record of disposal. This will include:

- Date item disposed of.
- Authorisation for disposal, including: verification of software licensing, any personal data likely to be held on the storage media.
- How it was disposed of e.g. waste, gift, sale.
- Name of person and/or organisation who received the disposed item.

Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

19. 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, the DPO 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

20. Training

All staff and governors are provided with data protection training as part of their induction process. All staff must also undertake annual refresher training.

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

21. Monitoring arrangements

The Data Protection Leads are responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the Resources and Personnel Committee of the Governing Body.

22. Legal framework and statutory 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 (DPA 2018)
- Keeping Children Safe in Education (current version)

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

Although the school does not currently use biometric data, if this changes, this policy meets the requirements of the Protection of Freedoms Act 2012 when referring to the use of biometric data.

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.

Linked policies/documents:

- CCTV Policy
- Use of IT agreement
- Privacy Notices
- Safeguarding Policy
- Freedom of Information Policy

23. Equalities & inclusion

The public sector equality duty consists of a general duty and specific duties. The general duty is set out in Section 149 of the Equality Act 2010 and it applies to public authorities such as schools when they are carrying out public functions. There is no explicit legal requirement under the general duty to collect and use equality information. However, to have due regard to the aims or needs of the general duty, public authorities must understand how their policies and practices affect those with particular protected characteristics.

Much of the personal data processed to comply with equality law is likely to be special category personal data. Special category personal information needs to be treated with greater care than other personal data and we must make sure that any personal information collected is necessary to meet our obligations under the general duty and be clear about how the information will be used.

As a result, where special category personal information is involved, we must satisfy:

- one of the special category conditions for processing; and
- one of the general conditions (which apply in every case).

These are set out in section 7 above.

In summary, we should take a proportionate approach and should always consider whether the same results could be achieved with fewer risks to privacy. We should also collect the minimum data required to achieve our objectives.

More information about the relationship between the public sector equality duty (PSED) and data protection law can be found here.

24. Safeguarding implications

The school holds significant amounts of personal and sensitive data about pupils, their families and staff. Compliance with this policy should reduce the risk of harm to pupils and staff caused by personal or sensitive data being shared inappropriately.

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 follow the schools Data Breach Procedure available on the staff website and notify the Data Protection Leads by email, providing as much detail as possible about the incident.
- The Data Protection Leads will investigate the report, and determine whether a breach has occurred. To decide, the Data Protection Leads 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 cooperate 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 Data Protection Leads will consider whether it is appropriate to alert the DPO, Headteacher and the chair of governors (this will depend on the scale/severity of the data breach)
- The Data Protection Leads will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the Data Protection Leads with this where necessary, and the Data Protection Leads should take external advice when required (e.g. from the DPO, IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The Data Protection Leads and, if appropriate, 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 Data Protection Leads 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 in the GDPR folder on Google Drive.
- 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 of the school's awareness of the breach. 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 or Data Protection Leads 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 and Data Protection Leads 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 Data Protection Leads will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - 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 the GDPR folder on Google Drive.
- The Data Protection Leads 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 Data Protection Leads and Headteacher will meet regularly 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 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.

For example:

Sensitive information being disclosed via email to unauthorized individuals (including safeguarding records)

- 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 Data Protection Leads as soon as they become aware of the error

If the sender is unavailable or cannot recall the email for any reason, the Data Protection Leads will ask the Network Manager to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the member of staff and/or Data Protection Leads will consider whether it's appropriate to 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 member of staff or Data Protection Leads will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request

- If appropriate the Data Protection Leads 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 Data Protection Leads will inform the DPO and designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners

A school laptop containing non-encrypted sensitive personal data is stolen or hacked

- The staff google account is suspended immediately

Hardcopy reports sent to the wrong pupils or families

- The sender should make contact with the individual who received it to explain that the information was sent in error, and request that those individuals return the information to the school and do not share, publish, save or replicate it in any way
- The member of staff or Data Protection Leads will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- If safeguarding information is compromised, the Data Protection Leads will inform the DPO and designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners