Data Protection Policy

COOMBE HOUSE
SCHOOL

Policy owner:	Quality Assurance Officer	**Adoption Date:** June 2023
Approved by company:	Finance, Audit and Risk Committee	
Review cycle:	Annual	
Last reviewed on:	February 2025	
Changes made:	Annual Review – wording changed from to align to all other policies. There are also additional sections on using Biometric Recognition Systems and Artificial Intelligence (AI). Email addresses have also been updated.	
Next review due by:	February 2026	

Dorset
Centre of
Excellence

Contents

1. Aims

Dorset Centre of Excellence (the Company) aims to ensure that all personal data collected about staff, children and young people, parents and carers, directors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This Data Protection Policy outlines how the Company protects personal data. Please see the notices listed below section 20 for more detail on what, how and why we process data in specific scenarios.

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 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

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.

It also takes into consideration the following legislation and guidance:

- Freedom of Information Act 2000 – including the Code of Practice 46 (FOIA).
- Public Records Act 1958.
- Limitation Act 1980.
- Inquiries Act 2005.
- Keeping Children Safe in Education statutory guidance for schools and colleges (May 2024).
- Working together to safeguard children statutory guidance.
- Guidance in the IRMS Information Management Toolkit for Schools.

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 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.

TERM	DEFINITION
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

The Company processes personal data relating to staff, directors, children and young people, parents and carers, visitors and others, and is therefore a data controller in relation to the processing activities where the Company determines the purposes and means for the data processing.

The Company is registered with the ICO, as legally required. The reference number is: ZB244508.

5. Roles and Responsibilities

This policy applies to **all staff** employed at Coombe House School (the 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 Board of Directors

The Board of Directors has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

5.2 Senior Responsible Individual (SRI)

The Company's Senior Responsible Individual (SRI) is the Managing Director who is contactable via the below details:
Dorset Centre of Excellence Limited
Donhead St Mary
Shaftesbury
SP7 9LP

Email: dpo@coombehouse.org.uk

The Quality Assurance Officer is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related procedures and guidelines where applicable. They are also the first point of contact for individuals whose data the Company processes, and for the ICO.

The Managing Director will report data protection issues directly to the Board of Directors and, where relevant, seek their advice and recommendations on company data protection issues.

5.3 Managing Director

The Managing Director 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 Company of any changes to their personal data, such as a change of address.
- Contacting the Quality Assurance Officer 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 the Company 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 Company 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 six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the company can fulfil a contract with the individual, or the individual has asked the company to take specific steps before entering into a contract.
- The data needs to be processed so that the company 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 company, 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 company (where the processing is not for any tasks that the company 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 child or young person) 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 child or young person) 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 child or young person) 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 personal data is collected directly from individuals, the relevant information required by data protection law will be provided to them.

Consideration will be given for the fairness of data processing. Personal data will not be handled 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

Personal data will only be collected for specified, explicit and legitimate reasons. These reasons will be explained to the individuals when first their data is first collected. Please refer to the following privacy notices for further details:

- Staff privacy notice.
- Parent and Pupil privacy notice.
- Visitor privacy notice.
- Website privacy notice.

If personal data is to be used for reasons other than those given when first obtained it, the individuals concerned will be informed beforehand, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

Data will be kept accurate and 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 company's data retention and disposal procedure and guidance.

8. Sharing Personal Data

Personal data should not be shared with anyone else without consent, but there are certain circumstances where it may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a child or young person or parent/carer that puts the safety of staff at risk.
- Suppliers or contractors need data to provide services to staff, children and young people – for example, IT companies. When doing this, the Company 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.

Personal data will be shared with law enforcement and government bodies when legally required to do so.

Personal data may also be shared with emergency services and local authorities to help them to respond to an emergency situation that affects any staff, children or young people.

Where personal data is transferred internationally, it will be done so in accordance with UK data protection law.

If a member of staff receives a request for the sharing of personal data, they should consult the Quality Assurance Officer for guidance.

9. Subject Access Requests and Other Rights of Individuals

9.1 Subject Access Requests (SARs)

Individuals have a right to make a 'subject access request' to gain access to personal information that the Company 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.

SARs can be submitted in any form, but preferably 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 Quality Assurance Officer.

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 SAR with respect to their child, the child must either be unable to understand their rights and the implications of a SAR 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 SAR. Therefore, most SARs from parents or carers of children or young people may be granted without the express permission of the child or young person. 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 to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of children and young people may not be granted without the express permission of the child or young person. This is not a rule and their 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, the Company:

- 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 (or receipt of the additional information needed to confirm identity, where relevant).
- Will provide the information free of charge.
- Where a request is complex or numerous, a response may be provided within three months. The individual will be informed of this within one month and explain why the extension is necessary. Please refer to the following ICO guidance as to whether a time extension would apply: What should we consider when responding to a request? | ICO.

Information may not be disclosed for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the child, young person 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 cannot reasonably be anonymised, and without the other person's consent, 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, then it may be refused, or charge a reasonable fee to cover administrative costs. It will be taken into account whether the request is repetitive in nature when making this decision.

When a request is refused, the individual will be informed of the reasons for this, and explain 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 SAR (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 consent to processing at any time.

- Request 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 Quality Assurance Officer. If staff receive such a request, they must immediately forward it to the Quality Assurance Officer.

10. Parental Requests to see the Educational Record (Coombe House School)

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 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. Biometric Recognition Systems

Where pupils biometric data as part of an automated biometric recognition system (for example, fingerprint identification or facial recognition used for unlocking electronic devices) the requirements of the Protection of Freedoms Act 2012, will be complied with.

Parents / carers will be notified before any biometric recognition system is put in place or before their child first takes part in it for any reason, other than to unlock an electronic device (see below). The School will get written consent from at least one parent / carer before any biometric data is taken from their child and first processed.

Parents / carers and pupils will be given information around the use of biometrics and should the pupil proceed with the use of fingerprints / facial recognition to unlock an electronic device, consent will be assumed. Should any parent / carer or pupil choose not to consent, electronic devices are able to be unlocked with a password of their choosing.

Parents / carers and pupils can withdraw consent, at any time, and any relevant data already captured will be deleted.

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

Where staff members use the biometric system(s), their consent will also be obtained before they first take part and provide alternative means of accessing the relevant service if they object. Staff can also withdraw consent at any time, and any relevant data already captured will be deleted.

12. CCTV

CCTV is used in various locations around the site to ensure it remains safe. The Company follows the ICO's guidance for the use of CCTV, and complies with data protection principles.

There is no requirement to ask individuals' permission to use CCTV, but it is made 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 Facilities and Health and Safety Manager.

Please refer to the company's CCTV procedure and guidance.

13. Photographs and Videos

As part of Company and School activities, photographs and images may be taken / recorded of individuals. Consent will always be requested prior to the photograph or recorded images being taken.

At Coombe House School, written consent is required from parents / carers for photographs and videos to be taken of their child for communication, marketing and promotional materials, evidence of learning/progress or for any other purpose. It will be clearly explained how the photograph and / or video will be used to both the parent / carer and the pupil.

Any photographs and videos taken by parents / carers at school events for their own personal use are not covered by data protection legislation. However, photos and / or videos with other pupils are not to be shared publicly on social media for safeguarding reasons, unless all the relevant parents / carers have agreed to this.

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

- On school notice boards and in school magazines, brochures, newsletters, etc.
- By external agencies such as the school photographer, newspapers, campaigns.
- On the School website or social media pages.
- To support evidence of learning and / or progress.

Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video will be removed where possible and not distributed further. However, printed photographs cannot be removed.

When using photographs and videos for purposes other than the evidence of learning and / or progress, personal information about the child or young person will not be included.

14. Artificial Intelligence (AI)

Artificial Intelligence 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 (Gemini). The School recognises that AI has may 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 too, the School 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

Measures are in place to show that data protection has been integrated into all of our data processing activities, including:

- Appointing a suitably qualified Senior Responsible Individual (SRI) and Quality Assurance Officer, 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 Company's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the Quality Assurance Officer will advise on this process).
- Conducting due diligence on all new suppliers that process personal data and ensuring that a data processing agreement is put in place.

- Integrating data protection into internal documents including this policy, any related policies / procedures and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies / procedures 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 ensure compliance.
- Appropriate safeguards being put in place if any personal data is transferred outside of the UK, where different data protection laws may apply.
- Maintaining records of processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our company and Senior Responsible Individual (SRI), and all information required to be shared about how personal data is used and process (via our privacy notices).
    - For all personal data held, maintaining an internal record of the type of data, type of data subject, how and why the data is being used, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how the data is kept secure.

16. Data Security and Storage of Records

Personal data will be protected and kept 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 paper based personal information needs to be taken off site, staff must sign it in and out from the company office.
- Staff and children and young people 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. Staff, children and young people or directors who store personal information on their personal devices are expected to follow the same security procedures as for company-owned equipment (see our online safety procedure). This should only be done with authorisation from the Senior Leadership team.

- Where personal data needs to be shared with a third party, due diligence is carried out and reasonable steps taken 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 it cannot or does not need to be rectified or updated.

For example, paper-based records will be shred, and electronic files overwritten or deleted. A third-party contractor is used to dispose of confidential paper waste who have provided sufficient guarantees that it complies with data protection law. There is a data processing agreement in place between the Company and the contractor to establish the responsibilities of each.

18. Personal Data Breaches

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

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

When appropriate, the data breach will be reported to the ICO within 72 hours after becoming aware of it. Such breaches 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 company laptop containing non-encrypted personal data about children or young people, staff or other individuals.

19. Training

All staff 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 Company's processes make it necessary.

20. Monitoring Arrangements

The Quality Assurance Officer is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the Finance, Audit and Risk Committee.

21. Privacy Notice

The Company provide privacy notices for parents and pupils, staff, visitors and website visitors in compliance with UK GDPR. Each privacy notice contains the following information:

- The categories of data held.
- Why the data is collected.
- The lawful basis on which that data is processed.
- Who the data is shared with.
- How long the data is retained for.
- An individuals right to access their personal data and the right to object.

The privacy notice for parents and pupils, visitors and website visitors are available on the School website. The staff privacy notice can be obtained from the Company office.

22. Links with Other Policies/Procedures

This data protection policy is linked to:

- Parent and Pupil Privacy Notice.
- Staff Privacy Notice.
- Visitor Privacy Notice.
- Website Privacy Notice.
- Data Retention and Disposal Procedure and Guidance.
- Online Safety Procedure.
- CCTV Procedure and Guidance.
- Information Security Procedure and Guidance.
- Safeguarding and Child Protection Policy.

All policies and procedures are available from the Company office. The contact details are listed below:

Email: office@coombehouse.org.uk

Telephone: 01747 449 84

23. Version Control

Date of adoption of this policy, by or on behalf of the Proprietor	June 2023
Date of last review of this policy	February 2025
Date for next review of this policy	February 2026
Policy owner (Proprietor)	Dorset Centre of Excellence

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, director or data processor must immediately notify the Quality Assurance Officer by emailingdpo@coombehouse.org.uk .
- The Quality Assurance Officer will investigate the report and determine whether a breach has occurred. To decide, the Quality Assurance Officer 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 persons.
- Staff and directors 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 Quality Assurance Officer will alert the Managing Director and the Headteacher .
- The Quality Assurance Officer will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the Quality Assurance Officer with this where necessary, and the Quality Assurance Officer should take external advice when required e.g., from IT providers. (See the actions relevant to specific data types at the end of this procedure).
- The Quality Assurance Officer 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 Quality Assurance Officer will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.
- The Quality Assurance Officer 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 company's computer system.

- Where the ICO must be notified, the Quality Assurance Officer 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 Company's awareness of the breach. As required, the Quality Assurance Officer 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 SRI.
    - 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 Quality Assurance Officer will report as much as they can within 72 hours of the Company's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the Quality Assurance Officer expects to have further information. The Quality Assurance Officer will submit the remaining information as soon as possible.
- Where the Company is required to communicate with individuals whose personal data has been breached, the Quality Assurance Officer 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 SRI.
    - 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 Quality Assurance Officer 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 Quality Assurance Officer will document each breach, irrespective of whether it is reported to the ICO. For each breach, records will be stored electronically and 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).

- The Quality Assurance Officer, Managing Director 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 Quality Assurance Officer, Managing Director and the Headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the company to reduce risks of future breaches.

Actions to minimise the impact of data breaches

The steps will be taken 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. The effectiveness of these actions will be reviewed and amended 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 Quality Assurance Officer as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the Quality Assurance Officer will ask the IT department to attempt to recall it from external recipients and remove it from the Company'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 Quality Assurance Officer should 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 Quality Assurance Officer will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The Quality Assurance Officer will carry out an internet search to check that the information has not been made public; if it has, the publisher / website owner or administrator will be contacted to request that the information is removed from their website and deleted.

- If safeguarding information is compromised, the Quality Assurance Officer will inform the Designated Safeguarding Lead and discuss whether the Company should inform any, or all, of its safeguarding partners.