Data Protection Policy

THE SPIRES COLLEGE

ADOPTED	September 2018
REVIEWED	March 2023
NEXT REVIEW	March 2024

Contents

1. **Aims** 3
2. **Legislation and Guidance** 3
3. **Definitions** 3
4. **The Data Controller** 4
5. **Roles and Responsibilities** 4
   - 5.1 Governing body 5
   - 5.2 Data protection officer 5
   - 5.3 All staff 5
6. **Data Protection Principles** 5
7. **Collecting Personal Data** 6
   - 7.1 Lawfulness, fairness and transparency 6
   - 7.2 Limitation, minimisation and accuracy 7
8. **Sharing Personal Data** 7
9. **Subject Access Request and other rights of individuals** 7
   - 9.1 Subject access requests 7
   - 9.2 Children and subject access requests 8
   - 9.3 Responding to subject access requests 8
   - 9.4 Other data protection rights of the individual 9
10. **Parental Requests to See the Educational Record** 9
11. **Biometric Recognition Systems** 10
12. **CCTV** 10
13. **Photographs and Video** 10
14. **Data Protection by Design and Default** 11
15. **Data Security and Storage of Records** 11
16. **Expectations of Staff** 12
17. **Disposal of Records** 12
18. **Training** 13
19. **Policy Monitoring and Review** 13
20. **Links with Other Policies** 13
21. **History of Changes** 13
22. **Appendix 1: Personal data breach procedure** 15

1. Aims

The Spires College aims to ensure that all personal data collected about staff, students, parents, 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 (DPA 2018)**

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

It meets the requirements of the **Protection of Freedoms Act 2012** when referring to our use of biometric data.

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

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

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.

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	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

The Spires College collects, processes and stores personal data relating to parents, students, staff, governors, visitors and others, and therefore is a 'data controller' for the purposes of data protection law. The Spires College is registered with the ICO under the Data Protection Act. Our registration number is ZA159941.

5. Roles and Responsibilities

This policy applies to **all staff** employed by The Spires College, 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 board has overall responsibility for ensuring that The Spires College complies with all relevant data protection obligations.

5.2 Data protection officer

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

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

Our DPO is Leanne Madge and is contactable via dpo@thespirescollege.com

5.3 All staff

Staff are responsible for:

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

6. Data Protection Principles

There are certain key data protection principles to which the College must have regard when processing personal data.

These are that personal data shall 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 Spires College 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 College can **fulfil a contract** with the individual, or the individual has asked the College to take specific steps before entering into a contract
- The data needs to be processed so that the College 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 College, 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 College (where the processing is not for any tasks the College 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 student) 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 student) 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 student) 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 College'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 student 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 Request 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 College 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 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 aged 12 and above are generally 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 students at our school may not be granted without the express permission of the student. This is not a rule and a student'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 two forms of identification
- May contact the individual via telephone 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
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one 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 student 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
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances). The erasure of personal data is also known as the Right to be Forgotten
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

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 student) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the College may charge a fee to cover the cost of supplying it.

This right applies as long as the student 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 student or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric Recognition Systems

Where we use students' biometric data as part of an automated biometric recognition system (*e.g. students use finger prints to receive school meals 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 College 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 students have the right to choose not to use the College's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can pay for school meals by using a PIN code.

Parents/carers and students 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 student 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).

Where staff members or other adults use the College'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.

Please see the College's **Protection of Biometric Information Policy** for further details.

12. CCTV

We use CCTV in various locations around the College 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.

Please see the College's **CCTV Policy** for further details.

13. Photographs and Video

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

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

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at College events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

Please see the College's **Photography and Video Consent, Use and Storage Policy** for further details.

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 where the College's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
- 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:

- Only authorised personnel can access, alter, disclose or destroy personal data
- Authorised personnel understand the limits of their authority and to whom they should escalate any issues relating to personal data;
- We have appropriate backup systems in place so that, if personal data is accidentally lost, altered or destroyed, it can be recovered
- Access to premises or equipment given to anyone outside the College (for example, for computer maintenance purposes) is strictly regulated and access to data limited
- We have proper procedures in place to identify individuals who are requesting personal data before it is given out
- There are strict guidelines in place on the appropriate use of computers to reduce the risk of the network being compromised
- We regularly review our physical security measures, such as ease of access to the premises through entrances and internal doors, alarm systems, lockable storage, security lighting and CCTV
- Portable IT equipment is appropriately encrypted so that data contained on such devices is secure

- Confidential paper files are not taken off site unless appropriate security measures have been implemented first
- 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 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. Expectations of Staff

We expect all staff working for, or on behalf of, The Spires College, whether employees, casual workers, supply staff, volunteers or consultants, to recognise and adhere to the high standards of data protection we uphold. Everyone has a responsibility for helping to ensure that personal data, whether their own or that of third parties, is accurate, kept up to date and held securely.

- Certain members of staff will collect and process data as part of their role. Without exception all members of staff must:
- Only access or process personal data they are authorised to as part of their role and in accordance with the documented purposes for processing (and not for any other purpose)
- Keep personal data confidential and only disclose it to individuals who are authorised to see it (if in any doubt, consulting their line manager or the Data Protection Officer)
- Not remove personal data from its authorised location without permission and, where permission is granted, to ensure that appropriate security measures are in place whilst the data is moved or relocated
- Not keep work-related personal data on personal devices, such as mobile phones and tablets, or on local computer hard drives or unencrypted USB sticks
- Take responsibility for ensuring that personal passwords are strong, are changed regularly and never shared
- Adhere to all security measures designed to keep personal data safe from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access
- Participate in training or briefings and read circulated documents aimed at increasing awareness of data protection legislation and good practice
- Be aware of data protection issues as part of their day-to-day work, particularly as part of any new projects, and report any concerns relating to personal data (including any potential data breaches) as a matter of urgency to the Data Protection Officer.

These rules are an integral part of The Spires College's data security practices in order to comply with data protection legislation. As such, a breach of these rules is likely to be treated as a disciplinary offence and potentially gross misconduct, in accordance with the disciplinary procedure.

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 College's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data is held and disposed of in accordance with the **IRMS Information Management Toolkit for Schools.**

18. 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 College's processes make it necessary.

19. Policy Monitoring and Review

The DPO is responsible for monitoring and reviewing this policy.

This policy is statutory and, as such, will be reviewed annually.

20. Links with Other Policies

This Data Protection Policy should be read in conjunction with the following College policies:

- CCTV Policy
- Photography and Video Consent and Storage Policy
- Protection of Biometric Information Policy
- ICT Acceptable Use Policy
- Electronic Communications Policy
- Network Security Policy
- Disciplinary Policy
- Staff Code of Conduct
- Safeguarding Policy

21. History of Changes

Date	Change	Where?
September 2021	Previous sections 'Introduction and Purpose of Policy' (1) and 'Policy Statement' (2) replaced with a clear statement of 'Aims'	Section 1
September 2021	New section: 'Legislation and Guidance'	Section 2
September 2021	Previous section 'Definitions and Principles (3) replaced with a more comprehensive glossary of definitions. Data Protection Principles now a separate section.	Section 3 Section 6
September 2021	New section explaining the role of the Data Controller	Section 4
September 2021	New section: Role and Responsibilities	Section 5
September 2021	Previous sections 'Our Approach to Processing Personal Data (4) and 'International Data Transfers' (6) replaced with two new sections 'Collecting Personal Data' and 'Sharing Personal Data'	Section 7 Section 8
September 2021	Previous section 'Rights of Individuals' replaced with new section 'Subject Access Request and other rights of individuals'	Section 9

September 2021	New section: 'Parental Requests to See the Educational Record'	Section 10
September 2021	New section: 'Biometric Recognition Systems'	Section 11
September 2021	New section: 'CCTV'	Section 12
September 2021	New section: 'Photography and Video'	Section 13
September 2021	Previous section 'Our Approach to Data Security and Breaches' (7) replaced with three new sections 'Data Protection by Design and Default', 'Data Security and Storage of Records' and 'Disposal of Records'	Section 14 Section 15 Section 16
September 2021	New section: 'Training'	Section 18
September 2021	Previous section 'Status of Policy and Review' (7) replaced with new section 'Monitoring Arrangements'	Section 19
September 2021	New Appendix: 'Personal data breach procedure'	Appendix 1
January 2023	Name of Data Protection Officer amended	Section 5

22. 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 data protection officer (DPO) by emailing **dpo@thespirescollege.com.**

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Staff and governors will 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 DPO will alert the Principal.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO 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 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.** It is important to report a suspected breach at the earliest possible opportunity even if the incident is downgraded to an event.

The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documesnted decisions are stored on the College's network.

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 College'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 College is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- 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 on the College's network.

The DPO and the Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

The DPO and the Principal 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 sensitive information being disclosed via email (including safeguarding records). We will review the effectiveness of these actions and amend them as necessary after any data breach.

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the Network Manager to attempt to recall it from external recipients and remove it from the College'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 DPO 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 DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

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