COTTESMORE SCHOOL

Data Protection Policy

This policy is addressed to all staff and explains the School's expectations of staff under data protection legislation. It provides an explanation of key data protection principles as well as detailed guidance on what to do in the event of a data breach.

Data protection is about regulating the way that the School uses and stores information about identifiable people (Personal Data). It also gives people various rights regarding their data - such as the right to access the Personal Data that the School holds on them.

As a school, we collect, store and process Personal Data about our staff, pupils, parents, suppliers and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in the School.

You are obliged to comply with this policy when processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action.

All queries concerning data protection matters should be raised with the Privacy and Compliance Officer.

Who does this policy apply to?

This policy is aimed at all staff working in the School (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities. It includes employees, governors, contractors, peripatetic tutors, work experience students and volunteers.

This policy does not form part of your contract of employment and may be amended by the School at any time.

What information falls within the scope of this policy?

Data protection concerns information about individuals.

Personal Data is data which relates to a living person who can be identified either from that data, or from the data and other information that is available. Information as simple as someone's name and address is their Personal Data.

In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data. Examples of places where Personal Data might be found are:

- on a computer database;
- in a file, such as a pupil report;
- a register or contract of employment;
- pupils' exercise books, coursework and mark books;
- health records; and
- email correspondence.

Examples of documents where Personal Data might be found are:

- a report about a child protection incident;
- a record about disciplinary action taken against a member of staff;
- photographs of pupils;
- a tape recording of an interview or meeting;
- contact details and other personal information held about pupils, parents and staff and their families;
- contact details of a member of the public who is enquiring about placing their child at the School;
- financial records of a parent;
- information on a pupil's performance; and
- an opinion about a parent or colleague in an email.

These are just examples - there may be many other things that you use and create that would be considered Personal Data.

You must be particularly careful when dealing with Personal Data which falls into any of the categories below:

- information concerning child protection matters;
- information about serious or confidential medical conditions and information about special educational needs;
- information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);
- financial information (for example about parents and staff);
- information about an individual's racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- genetic information;

- information relating to actual or alleged criminal activity; and
- biometric information (e.g. a pupil's fingerprints following a criminal investigation).

These categories are referred to as special categories of personal data in this policy. If you have any questions about your processing of these categories of Personal Data please speak to the Privacy and Compliance Officer.

Your obligations

Personal Data must be processed fairly, lawfully and transparently.

"Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.

People must be told what data is collected about them, what it is used for and who it might be shared with, unless it is obvious. They must also be given other information, such as what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (the data protection regulator).

This information is often provided in a document known as a privacy notice or a transparency notice. Copies of the School's privacy notices can be accessed on the School's website. You must familiarise yourself with the School's privacy notices.

If you are using Personal Data in a way which you think an individual might think is unfair please speak to the Privacy and Compliance Officer.

You must only process Personal Data for the following purposes:

- ensuring that the School provides a safe and secure environment;
- providing pastoral care;
- providing education and learning for our pupils;
- providing additional activities for pupils and parents (for example activities and clubs);
- protecting and promoting the School's interests and objectives (for example fundraising);
- safeguarding and promoting the welfare of our pupils; and
- to fulfil the School's contractual and other legal obligations.

If you want to do something with Personal Data that is not on the above list, or is not set out in the relevant privacy notice(s), you must speak to the Privacy and Compliance Officer. This is to make sure that the School has a lawful reason for using the Personal Data.

We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you should speak to the Privacy and Compliance Officer if you think that you may need to obtain consent.

You must only process Personal Data for limited purposes and in an appropriate way

For example, if pupils are told that they will be photographed to enable an external examiner to recognise them, you should not use those photographs for another purpose (e.g. in the School's prospectus). Personal Data held must be adequate and relevant for the purpose.

This means not making decisions based on incomplete data. For example, when writing reports you must make sure that you are using all of the relevant information about the pupil. You must not hold excessive or unnecessary Personal Data.

Personal Data must not be processed in a way that is excessive or unnecessary. For example, you should only collect information about a pupil's siblings if that Personal Data has some relevance, such as allowing the School to determine if a sibling fee might be permissible. The Personal Data that you hold must be accurate.

You must ensure that Personal Data is complete and kept up to date. For example, if a parent notifies you that their contact details have changed, you should update the School's information management system. You must not keep Personal Data longer than necessary.

The School has a Storage and Retention of Records and Documents Policy which gives details of how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data.

Please speak to the Privacy and Compliance Officer for guidance on the retention periods and secure deletion processes. You must keep Personal Data secure.

You must comply with the following School policies and guidance relating to the handling of Personal Data:

- IT Acceptable Use Policy;
- CCTV Policy;
- Mobile Phone and Camera Policy;
- Taking, Storing and Using Images of Children Policy;
- Drone Policy;
- Storage and Retention of Records and Documents Policy;

You must not transfer Personal Data outside the EEA without adequate protection.

If you need to transfer Personal Data outside the EEA please contact the IT Manager. For example, if you are arranging a school trip to a country outside the EEA.

Sharing Personal Data outside the School - dos and don'ts

Please review the following dos and don'ts:

- DO share Personal Data on a need to know basis and think about why it is necessary to share data outside of the School. If in doubt always ask your manager, the Privacy and Compliance Officer or in matters relating to a pupil's well-being, the Designated Safeguarding Lead.
- DO NOT send emails which contain special categories of personal data described above without taking steps to ensure that the data cannot be accessed by anyone other than the intended recipient.
- DO make sure that you have permission from your manager or the Privacy and Compliance Officer to share Personal Data on the School website.
- DO be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You should seek advice from the Privacy and Compliance Officer where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from a parent but using a different email address).
- DO be aware of "phishing". Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the IT Manager.
- DO NOT disclose Personal Data to the Police without permission from the Privacy and Compliance Officer (unless it is an emergency, in which case seek the Headmaster's permission where possible).
- DO NOT disclose Personal Data to contractors without permission from the Privacy and Compliance Officer.

Sharing Personal Data within the School

This section applies when Personal Data is shared within the School.

Personal Data must only be shared within the School on a "need to know" basis.

Examples of sharing which are likely to be compliant with data protection legislation include:

- a teacher discussing a pupil's academic progress with other members of staff (for example, to ask for advice on how best to support the pupil);
- informing an exam invigilator that a particular pupil suffers from panic attacks; or
- disclosing details of a teaching assistant's allergy to bee stings to colleagues so that you/they will know how to respond (but more private health matters must be kept confidential).

Examples of sharing which are unlikely to be compliant with data protection legislation include:

- the Head of Finance and Operations being given access to all pupil records kept by the Surgery (seniority does not necessarily mean a right of access);
- informing all staff that a pupil has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil); or
- disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff (unless the member of staff has given permission or it is an emergency).

You may share Personal Data to avoid harm, for example in child protection and safeguarding matters. You should have received training on when to share information regarding welfare and safeguarding issues. If you have not received this training please contact the Designated Safeguarding Lead or the Headmaster.

Individuals' rights in their Personal Data

People have various rights in their information.

You must be able to recognise when someone is exercising their rights so that you can refer the matter to the Privacy and Compliance Officer. Please let them know if anyone (either for themselves or on behalf of another person, such as their child):

- wants to know what information the School holds about them or their child;
- asks to withdraw any consent that they have given to use their information or information about their child;
- wants the School to delete any information;
- asks the School to correct or change information (unless this is a routine updating of information such as contact details);

- asks for electronic information which they provided to the School to be transferred back to them or to another organisation;
- wants the School to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the School newsletter or Old Cottesmorians events information; or
- objects to how the School is using their information or wants the School to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

Requests for Personal Data (Subject Access Requests)

One of the most commonly exercised rights mentioned above is the right to make a subject access request. Under this right people are entitled to request a copy of the Personal Data which the School holds about them (or in some cases their child) and to certain supplemental information.

Subject access requests do not have to be labelled as such and do not even have to mention data protection. For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid subject access request. You must always immediately let the Privacy and Compliance Officer know when you receive any such requests.

Receiving a subject access request is a serious matter for the School and involves complex legal rights. Staff must never respond to a subject access request themselves unless authorised to do so.

When a subject access request is made, the School must disclose all of that person's Personal Data to them which falls within the scope of his/her request. There are only very limited exceptions. There is no exemption for embarrassing information so think carefully when writing letters and emails as they could be disclosed following a subject access request. However, this should not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to safeguarding matters.

Data breaches

The School understands the importance of keeping Personal Data secure and of effectively dealing with data breaches. This is essential for maintaining the trust of staff, pupils and their parents when the School uses their information.

This policy and procedure is to be used by the Privacy and Compliance Officer in the event of a data breach at the School (or a suspected data breach). The Privacy and Compliance Officer will work with the senior leadership team to deal with the different aspects of a data breach.

The School is required to report certain breaches to the Information Commissioner's Office and to data subjects under the General Data Protection Regulation. There are strict timescales for reporting breaches. This policy gives more information about how the School will ensure that timely and compliant reports are made.

What is a data breach?

A data breach is a breach of security which leads to any of the following:

- the loss of Personal Data;
- the accidental or unlawful destruction of Personal Data;
- the disclosure of Personal Data to an unauthorised third party;
- the unlawful or accidental alteration of Personal Data; or
- unauthorised access to Personal Data.

If staff are in any doubt as to whether an incident constitutes a data breach they must speak to the Privacy and Compliance Officer immediately.

Immediate action following a data breach

➢ Inform the Privacy and Compliance Officer

➢ Identify what Personal Data is at risk

➢ Take measures to prevent the breach from worsening e.g. changing password/access codes, removing an email from pupils' inboxes which was sent by mistake.

➢ Recover any of the compromised Personal Data e.g. use back-ups to restore data.

➢ Consider whether outside agencies need to be informed as a matter of urgency e.g. the police in the event of a burglary or Children's Services where the breach may lead to serious harm being caused to a pupil.

➢ Consider whether any affected individuals should be told about the breach straight away e.g. so that they may take action to protect themselves or because they would find out about the breach from another source.

Roles and responsibilities

The following staff and have certain responsibilities:

Role	Responsibility
Privacy and Compliance Officer (PCO)	The PCO will chair the Breach Response Group and is responsible for co-ordinating the School's response to any breach. In addition, the PCO will lead on any physical security measures which are required at the School site to contain the breach. The PCO is responsible for notifying and liaising with the School's insurers as required. The PCO will lead on any employee welfare or disciplinary issues in consultation with the Headmaster
Headmaster	The Headmaster will be responsible for any communications with pupils and parents and for any pupil welfare or disciplinary considerations.
IT Manager	The IT Manager will be responsible for ensuring the security of the School's IT infrastructure. In addition, for taking any possible technical measures to recover Personal Data or to contain a data breach.
Proprietor	The Proprietor will be responsible for liaising with the Governing Advisors

Containment and recovery

As soon as a data breach has been identified or is suspected, the School will take steps to recover any Personal Data and to contain the breach, which may include:

- change any passwords and access codes which may have been compromised;
- if appropriate in all the circumstances, tell employees to notify their bank if financial information has been lost (or other information which could lead to financial fraud);
- limit staff and/or pupil access to certain areas of the School's IT network;
- use back-up tapes to restore lost or damaged data;
- take any measures to recover physical assets e.g. notifying the police or contacting third parties who may have found the property;
- notify insurers; and
- take action to mitigate any loss.

The Breach Response Group will decide what action is necessary and which member(s) of the Group will be responsible for the different aspects of the containment and recovery. Where appropriate the Group may delegate tasks to other members of staff with the relevant expertise.

The Group may seek assistance from outside experts if appropriate to effectively contain the breach and recover any Personal Data e.g. legal advice, reputation management advice or specialist technical advice. Establishing and assessing the risks.

The next stage in the process of dealing with a data breach is to establish and assess the risks presented by the breach. The Group's approach will be shaped by the questions set out in the Appendix to this policy.

Notification

The School is required to report a data breach to the ICO unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The Group's risk assessment will be used to determine if a notification to the ICO is required, and the reasons for a decision not to notify the ICO will be documented by the Group. A notification to the ICO will be made without undue delay and where feasible within 72 hours of having become aware of the breach.

The School will observe ICO procedures for data breach notifications https://ico.org.uk/for-organisations/report-a-breach/. The School may also prepare a letter to the ICO in addition to following the ICO's procedures in order to set the context for the breach.

The School's notification will contain as a minimum:

- a description of the nature of the data breach including where possible:
- the categories and approximate number of data subjects concerned; and
- the categories and approximate number of Personal Data records concerned;
- the name and contact details of the Privacy and Compliance Officer who can provide more information to the ICO if required;
- a description of the likely consequences of the data breach;
- a description of the measures taken or proposed to be taken by the School to address the data breach, including where appropriate measures to mitigate its possible adverse effects.

If it is not possible to submit the notification to the ICO within 72 hours of becoming aware of the breach, the School will explain the reason for this delay.

If it is not possible to provide all of the information at the same time, the School will provide the information to the ICO in phases without further undue delay. For example, the School may make an initial notification within the 72 hour period with a more detailed response the following week once the School has more information on what happened.

The School will also consider reporting the data breach to the Police, where it is possible that a criminal offence has been committed.

Contacting affected individuals

The School is required by the GDPR to report a data breach to the individuals whose data has been compromised (known as data subjects) where the breach is likely to result in a high risk to the rights and freedoms of individuals. It may not always be clear which individuals should be notified, for example, parents may need to be notified rather than their children.

A notification does not need to be made where:

- the School had taken measures so that the data compromised was unintelligible to any person not authorised to access it (e.g. it was encrypted); or
- the School has managed to contain the breach or take mitigating action so that any high risk to individuals is no longer likely to materialise (e.g. an unencrypted memory stick has been recovered before anyone was able to access the data held on it).

If the School decides not to notify individuals this decision will be documented.

If a notification is sent this will be done without undue delay. The Group will decide what is the most appropriate method of communication for the notification, and factors to consider include the urgency of the notification. For example, it may be appropriate to telephone individuals followed up with an email.

The School may work with external agencies, including the ICO and the Police to determine when is the most appropriate time to notify the individuals. The ICO may advise or require the School to notify individuals. In addition, the ICO has the authority to require a more detailed notification to be given to individuals.

Notifications to individuals will include the following as a minimum:

- the name and contact details of a person at the School who can provide more information. The Group should choose the appropriate staff member at the School, which is likely to depend upon which individuals are affected;
- a description of the likely consequences of the data breach; and
- a description of the measures taken or proposed to be taken by the School to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In addition, the School will consider if any additional information would be helpful to data subjects. For example, instructions on measures which they can take to protect their data now or in the future.

Internal Breach Register

The School is required to keep a register of all data breaches including those which do not meet the threshold to be reported. Staff are regularly trained to report all data breaches to allow the School to meet this requirement.

The Privacy and Compliance Officer is responsible for keeping this register up to date.

Evaluation

The School regularly evaluates of the effectiveness of both its organisational and technical measures to protect Personal Data.

Organisational measures include:

- policies for staff on their data protection obligations, including when working away from the School site;
- guidance for staff on how to use specific computer applications and software securely; and
- data protection training for staff.

Technical measures include:

- the use of encryption;
- limiting access to certain areas of the School's IT network;
- firewalls and virus protection; and
- the use of backups.

The Group will establish how existing measures could be strengthened and what additional measures should be put in place to guard against future data breaches. The Group will consider both breaches of a similar type to that which has occurred and the risk of security breaches more broadly. The Group may delegate this task to one or more appropriate members of staff and will consider whether legal and/or technical advice is required.

Key points for the evaluation to consider include:

- Was the breach reported to the Privacy and Compliance Officer immediately? If not, what action can be taken to speed up the process of contacting a senior member of staff?
- Were all possible measures taken to recover the data promptly?
- Could more have been done to contain the breach as quickly as possible?
- If one of the School's processors (e.g. a payroll supplier) was either responsible for the breach, or discovered the breach, was this notified to the School without undue delay? If not, what measures can be put in place to improve this communication in the future?

- Would improvements in the training given to staff have prevented the breach or lessened the severity of the breach?
- Can measures be taken to speed up the process of staff reporting breaches?
- Do any of the School's policies need to be revised?
- Are changes required to the School's IT system?
- Should the School's document management system be made more robust? For example, should staff's ability to access certain documents be limited to a greater extent.
- Does the physical security of the School, particularly in areas where Personal Data is kept, need to be improved? D
- Do the School's remote working practices need to change?
- Does the School need more robust procedures around staff using their own devices for School work?
- Do the School's contracts with processors need to be revised?
- Does the School need to do more robust due diligence on its processors?

The Group will report the outcome of the evaluation to the Proprietor and Governing Advisors before implementing any necessary changes.

Breach of this policy

Any breach of this policy will be taken seriously and may result in disciplinary action.

A member of staff who deliberately or recklessly discloses Personal Data held by the School without proper authority is guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

COTTESMORE SCHOOL

Data Protection Policy – Appendix

Establishing and Assessing the Risks Presented by a Data Breach

No.	Question	Response
1	Precisely what data has been (or is thought to have been) lost, damaged or compromised?	
2	Is any of the data special categories of personal data as defined in the School's Data Protection Policy? This would be: i. information concerning child protection matters; ii. information about serious or confidential medical conditions and information about special educational needs; iii. information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved); iv. financial information (for example about parents and staff); v. information about an individual's racial or ethnic origin; vi. political opinions; vii. religious beliefs or other beliefs of a similar nature; viii. trade union membership; ix. physical or mental health or condition; x. genetic information; xi. sexual life; xii. information relating to actual or alleged criminal activity; or xiii. biometric information (e.g. a pupil's fingerprints following a criminal investigation). **If any of these types of data are involved this makes the breach more serious.**	

3	Who are the affected individuals e.g. staff, parents, pupils, third parties?	
4	How many individuals have definitely been affected? How many are potentially affected (worst case scenario)?	
5	What harm might be caused to individuals (not to the School)? The individuals do not necessarily need to be those who's Personal Data was involved in the breach. Harm should be interpreted broadly, for example to include: i. distress ii. discrimination; iii. loss of confidentiality; iv. financial damage; v. identity theft; vi. physical harm; vii. reputational damage	
6	What harm might be caused to the School? For example, reputational damage and financial loss.	
7	What mitigating factors may have lessened the risks presented by the breach? The following questions may assist when considering this point: i. Were any physical protections in place to limit the impact of the breach e.g. was the data contained in a locked case when it was lost/stolen? ii. Were any technical protections in place e.g. was the data protected by encryption or pseudonymisation? iii. Have measures been taken to contain the breach e.g. have banks being notified where financial information has been compromised? iv. Have measures been taken to recover the data e.g. has lost data been found before being seen by any unauthorised party or have back-ups been used where electronic information was lost or damaged?	
8	If the Group determines not to notify the ICO of the data breach, record here the reasons for that decision.	