Reviewed and Approved by the Governing Council: Summer 2024
Next Review: Summer 2025
Responsibility: Data Manager

Data Protection Policy

Introduction

1. **Introduction**: This policy is about your obligations and rights under the data protection legislation. Data protection is about regulating the way that the College uses and stores information about identifiable people (Personal Data). Data protection legislation also gives people various rights regarding their data - such as the right to access a copy of the Personal Data that the College holds on them.

2. **Lawful treatment of data:** As a school, we will 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 College and will ensure that the College operates successfully.

3. **Additional Information:** In addition to this policy, you must also read the following which are relevant to data protection:

   3.1 the College's privacy notices;

   3.2 IT acceptable use policy for staff;

   3.3 retention of Data and Requesting Erasure of Personal Information policy

   3.4 Access and Security policy; and

   3.5 Taking, Storing and Using Images of Pupils policy.

4. **Application:** This policy applies to all staff working in the School (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities. This includes employees, governors, contractors, agency staff, work experience / placement students and volunteers.

5. **Obligation:** You must comply with this policy when processing Personal Data on the College's behalf. Any breach of this policy may result in disciplinary action. This policy does not form part of your contract of employment and may be amended by the School at any time.

6. **Queries:** The Bursar is responsible for helping you to comply with the College's obligations. All queries concerning data protection matters should be raised with the Bursar.

Scope of this Policy

7. **Data Protection**: Data protection concerns information about individuals.

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

9. **Personal Data at work:** In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data.

10. Examples of places where Personal Data might be found are:

10.1 on a computer database;

10.2 in a file, such as a pupil report;

10.3 a register or contract of employment;

10.4 pupils' exercise books, coursework and mark books;

10.5 health records; and

10.6 email correspondence.

11. Examples of documents where Personal Data might be found are:

11.1 a report about a child protection incident;

11.2 a record about disciplinary action taken against a member of staff;

11.3 photographs and videos of pupils;

11.4 a tape recording of a job interview;

11.5 contact details and other personal data held about pupils, parents and staff and their families;

11.6 contact details of a member of the public who is enquiring about placing their child at the College;

11.7 financial records of a parent;

11.8 information on a pupil's performance; and

11.9 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.

12. **Critical College Personal Data:** The following categories are referred to as **Critical College Personal Data** in this policy. Critical College Personal Data is information which concerns:

12.1 safeguarding or child protection matters;

12.2 serious or confidential medical conditions;

12.3 special educational needs;

12.4 financial information including parent and staff bank details;

12.5 an individual's racial or ethnic origin;

12.6 political opinions;

12.7 religious beliefs or other beliefs of a similar nature;

12.8 trade union membership;

12.9 someone's physical or mental health or condition;

12.10 sex life or sexual orientation;

12.11 actual or alleged criminal activity, criminal convictions, or the absence of criminal convictions (e.g. Disclosure and Barring Service checks);

12.12 allegations made against an individual (whether or not the allegations amount to a criminal offence and whether or not the allegations have been proved);

12.13 biometric information used for the purpose of uniquely identifying someone (for example fingerprints used for controlling access to a building); and

12.14 genetic information.

If you have any questions about your processing of these categories of Critical College Personal Data please speak to the Bursar.

13. **Sharing information in a mental health emergency:** in the event of a mental health emergency, the College may need to share certain Critical College Personal Data in order to ensure the safety and wellbeing of the member of staff involved. Data protection law does not prevent the sharing of necessary and proportionate information in such emergencies. Any information shared during a mental health emergency will be handled securely and shared only with those who need to know. The College will take all necessary steps to protect the confidentiality and integrity of the data being shared. The College asks that you keep your next of kin and emergency contact details up to date. Regular reviews will be conducted to ensure the accuracy of this information.

Your Obligations

14. Personal Data must be processed fairly, lawfully and transparently

14.1 What does this mean in practice?

14.1.1 "Processing" covers virtually everything which is done with Personal Data, including using, sharing (internally or externally), copying and storing Personal Data.

14.1.2 People must be told what data is collected about them, what it is used for, and who it might be shared with. 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).

14.2 This information is provided in a document known as a privacy notice. Copies of the College's privacy notices can be obtained from the Bursar's PA or accessed on the College's website. You must familiarise yourself with the College's privacy notices, including those for pupils, parents and Staff.

14.3 If you are using Personal Data in a way which someone might reasonably think is unfair please speak to the Bursar.

15. You must only process Personal Data for the following purposes:

15.1 ensuring that the School provides a safe and secure environment;

15.2 providing pastoral care including safeguarding, child protection and promoting the welfare of our pupils;

15.3 making sure that the School is a good place to work and in relation to HR and staff matters;

15.4 providing education and learning for our pupils;

15.5 providing additional activities for pupils and parents (for example, activity clubs);

15.6 protecting and promoting the School's interests and objectives (for example, fundraising and commercial ventures); and

15.7 to fulfil the School's contractual and other legal obligations.

16. **Use of Personal Data:** 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 Bursar. This is to make sure that the College can lawfully use the Personal Data.

17. **Consent:** We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you must speak to the Bursar if you think that you may need to seek consent. If you are not an employee of the College (for example, if you are a volunteer), then you must be extra careful to make sure that you are only using Personal Data in a way that has been expressly authorised by the College.

18. **You must have a good reason to use personal data**

18.1 What does this mean in practice?

18.1.1 You must only use personal Data for specified, explicit and legitimate purposes and not use personal data in a way that is incompatible with these purposes. For example, if pupils are told that they will be photographed to enable staff to recognise them when writing references, you must not use those photographs for another purpose (e.g. in the School's prospectus). Please see the School's Taking, storing and using images of pupils policy for Staff on the Use of Photographs and Videos for further information relating to the use of photos and videos.

19. Personal Data held must be adequate and relevant for the purpose

19.1 What does this mean in practice?

19.1.1 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.

20. You must not hold excessive or unnecessary Personal Data

20.1 What does this mean in practice?

20.1.1 Personal Data must not be processed in a way that is excessive or unnecessary. For You must limit the Personal Data that you collect or use to the minimum needed to meet your objectives. For example, you must 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 discount is applicable.

21. The Personal Data that you hold must be accurate

21.1 What does this mean in practice?

21.1.1. 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 must ensure that the College's information management system has been updated and, as good practice, inform staff who you know have regular contact with the parent.

22. You must not keep Personal Data longer than necessary

22.1 What does this this mean in practice?

22.1.1 The College has a policy about 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 and must check the policy before doing so. You must only delete Personal Data if you are authorised to do so.

22.1.2 Please speak to the Bursar for guidance on the retention periods and secure deletion.

23. You must keep Personal Data secure

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

(a) Policy for Staff on the Taking, storing and using images of pupils by the College;

(b) IT acceptable use policy for staff; and

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

24.1 What does this mean in practice?

24.1.1. If you need to transfer Personal Data outside the UK or the EEA please contact the Data Manager. For example, if you are arranging a College trip to a country outside the EEA.

25. **Accountability**

25.1 The College is responsible for and must be able to demonstrate compliance with the data protection principles. You are responsible for understanding your particular responsibilities under this policy to help ensure we meet our accountability requirements.

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

26. **Dos and don'ts**: Please review the following dos and don'ts:

26.1 DO share Personal Data on a need-to-know basis only - think about why it is necessary to share data outside of the College - if in doubt - always ask your manager.

26.2 DO encrypt emails which contain Critical College Personal Data described in paragraph 12 above. For example, encryption must be used when sending details of a safeguarding incident to social services.

26.3 DO make sure that you have permission from your Manager to share Personal Data on the College website or using the College's social media accounts.

26.4 DO check with your Manager before using an app or other software that has not been authorised by the College.

26.5 DO share Personal Data in accordance with the College's Safeguarding Policy. If you have any questions or concerns relating to safeguarding, you must contact the Designated Safeguarding Lead.

26.6 DO be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You must seek advice from the Bursar 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).

26.7 DO be aware of phishing. Phishing is a type of attack in which attackers attempt to deceive individuals into providing sensitive information, for example, 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 or if you have any concerns about the message. You must report all concerns about phishing to the IT department immediately.

26.8 DO NOT disclose Personal Data to the police without permission from the Bursar (unless it is an emergency).

26.9 DO NOT disclose Personal Data to contractors without permission from the Bursar. This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil recruitment event.

Accessing or sharing Personal Data within the College

27. **Sharing Personal Data:** This section applies when Personal Data is accessed or shared within the College.

28. **Need to know basis:** Personal Data must only be accessed or shared within the College on a "need to know" basis.

Examples which are likely to comply with data protection legislation:

28.1 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);

28.2 sharing Personal Data in accordance with the College's safeguarding policy;

28.3 informing an exam invigilator that a particular pupil suffers from panic attacks; and

28.4 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 which are unlikely to comply with data protection legislation:

28.5 the Head being given access to all records kept by nurses working within the College (seniority does not necessarily mean a right of access);

28.6 a member of staff looking at a colleague's HR records without good reason. For example, if they are being nosey or suspect their colleague earns more than they do. In fact, accessing records without good reason can be a criminal offence (see paragraph 37 below);

28.7 informing all staff that a pupil has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil); and

28.8 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).

29. **Sharing of Personal Data and safeguarding:** 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 as a matter of urgency.

Individuals' rights in their Personal Data

30. **Rights:** 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 Bursar. These rights can be exercised either in writing (e.g. in an email) or orally.

31. **Individual's rights:** Please let the Bursar know without delay if anyone (either for themselves or on behalf of another person, such as their child):

31.1 wants a copy of the Personal Data the School holds about them or their child. This is commonly known as a subject access request;

31.2 asks to withdraw any consent that they have given to use their Personal Data or information about their child;

31.3 wants the School to delete any Personal Data;

31.4 asks the school to correct or change Personal Data (unless this is a routine updating of information such as contact details);

31.5 asks for Personal Data to be transferred to them or to another organisation;

31.6 wants the school to stop using their Personal Data for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the School newsletter or alumni events information;

31.7 objects to how the School is using their Personal Data or wants the School to stop using their Personal Data in a particular way, for example, if they are not happy that Personal Data has been shared with a third party ; or

31.8 exercises their right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

32. Please note, a person may be committing a criminal offence if they alter, block, erase, destroy or conceal information to prevent it from being disclosed (for example, to prevent its disclosure if a subject access request for that information has been received). Therefore, if you are asked to provide information or documents to a colleague at the College who is preparing a response to a request for information then you must make sure that you provide everything.

Requests for Personal Data (Subject Access Requests)

33. **The right to request Personal Data:** One of the most commonly exercised rights mentioned in section 29 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 College holds about them (or in some cases their child) and to certain supplemental information.

34. **Form of request:** 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 Bursar know when you receive any such requests.

35. **If you receive a Subject Access Request:** Receiving a Subject Access Request is a serious matter for the College and involves complex legal rights. Staff must never respond to a Subject Access Request themselves unless authorised to do so.

36. **Disclosure:** When a Subject Access Request is made, the College must disclose all of that person's Personal Data to them which falls within the scope of their request - there are only very limited exceptions. There is no exemption for unprofessional comments or embarrassing information - so think carefully when writing comments about people as they could be disclosed following a Subject Access Request. However, this must not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to safeguarding matters.

Breach

37. **Breach:** A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.

38. **Criminal offence:** A member of staff who deliberately or recklessly obtains or discloses Personal Data held by the College (or procures its disclosure to another person) without proper authority is also guilty of a criminal offence. In some cases, it can also be an offence to re-identify information which has been de-identified. Please speak to the Bursar before doing this.