THE KING'S SCHOOL IN MACCLESFIELD

DATA PROTECTION POLICY

Introduction

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

1. **Lawful treatment of data**: As a school, we will collect, store and process Personal Information about our staff, pupils, parents, suppliers and other third parties. We recognise that the correct and lawful treatment of this information will maintain confidence in the School and will ensure that the School operates successfully.

2. **Application**: 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, which includes employees, governors, contractors, agency staff, work experience / placement, students and volunteers.

3. **Obligation**: You are obliged to comply with this policy when processing Personal Information on our behalf. Any breach of this policy may result in disciplinary action.

4. **Queries**: The Data Protection Officer (Director of Finance) is responsible for helping you to comply with the School's obligations. All queries concerning data protection matters should be raised with the Data Protection Officer.

What information falls within the scope of this policy

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

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

7. **Personal Information at work:** In order for you to do your job, you will need to use and create Personal Information. Most items relate to a pupil or their parents.

Examples of places where Personal Information might be found are:

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

- health records; and
- email correspondence.

Examples of documents where Personal Information 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 a job interview or disciplinary hearing;
- 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 Information.

8. **Categories of Critical School Personal Information:** The following categories are referred to as **Critical School Personal Information** in this policy. You must be particularly careful when dealing with Personal Information, which falls into any of the categories below:

    8.1 information concerning child protection matters;

    8.2 information about serious or confidential medical conditions and information about special educational needs;

    8.3 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);

    8.4 financial information (for example about parents and staff);

    8.5 information about an individual's racial or ethnic origin;

    8.6 political opinions;

    8.7 religious beliefs or other beliefs of a similar nature;

    8.8 trade union membership;

    8.9 physical or mental health or condition;

    8.10 sex life or sexual orientation;

    8.11 genetic information;

    8.12 information relating to actual or alleged criminal activity; and

    8.13 biometric information (e.g. a pupil's fingerprints following a criminal investigation).

If you have any questions about your processing of these categories of Critical School Personal Information please speak to the Data Protection Officer.

Your obligations

9. **Personal Information must be processed fairly, lawfully and transparently.**

9.1 What does this mean in practice?

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

9.1.2 People must be told what information 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).

9.2 This information is often provided in a document known as a Privacy Notice. Copies of the School's Privacy Notice is available of the school's website or from the Data Protection Officer.

9.3 If you are using Personal Information in a way which you think an individual might think is unfair please speak to the Data Protection Officer.

10. **You must only process Personal Information for the following purposes:**

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

10.2 providing pastoral care;

10.3 providing education and learning for our pupils;

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

10.5 protecting and promoting the School's interests and objectives (for example fundraising);

10.6 safeguarding and promoting the welfare of our pupils; and

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

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

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

13. **You must only process Personal Information for specified, explicit and legitimate purposes:**

For example, if pupils are told that they will be photographed to enable staff to recognise them when writing references, you should not use those photographs for another purpose (e.g. in the School's prospectus). Please see the School's Code of Conduct and the guidance for staff on the use of photographs and videos of pupils by the School for further information relating to the use of photographs and videos.

14. **Personal Information held must be adequate and relevant for the purpose:**

    This means not making decisions based on incomplete information. For example, when writing reports you must make sure that you are using all of the relevant information about the pupil.

15. **You must not hold excessive or unnecessary Personal Information:**

    Personal Information 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 Information has some relevance, such as [• allowing the School to determine if a sibling fee discount is applicable].

16. **The Personal Information that you hold must be accurate**:

    You must ensure that Personal Information 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.

17. **You must not keep Personal Information longer than necessary**:

    The School 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 information. Please speak to the Data Protection Officer for guidance on the retention periods and secure deletion.

18. **You must keep Personal Information secure**:

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

    Guidance for staff on the use of photographs and videos of pupils by the school; and

    IT acceptable use policy for Staff;

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

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

    19.1 **DO** share Personal Information on a need to know basis - think about why it is necessary to share information outside of the School - if in doubt - always ask your line manager or senior member of staff.

    19.2 **DO** encrypt emails which contain Critical School Personal Information described in paragraph above. For example, encryption should be used when sending details of a safeguarding incident to social services.

    19.3 **DO** make sure that you have permission from your line manager to share Personal Information on the School website.

    19.4 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Information from people or organisations. You should seek advice from Data Protection 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).

19.5 **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 department.

19.6 **DO NOT** disclose Personal Information to the police without permission from The Data Protection Officer (unless it is an emergency).

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

Accessing or Sharing Personal Information within the School

20. **Sharing Personal Information:** This section applies when Personal Information is accessed or shared within the School.

21. **Need to know basis**: Personal Information must only be accessed or shared within the School on a "need to know" basis.

Examples , which are **likely** to comply with data protection legislation:

21.1 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);

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

21.3 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:

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

21.5 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.

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

21.7 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).

22. **Sharing of Personal Information and safeguarding:** You may share Personal Information 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 Designated Safeguarding Lead as a matter of urgency.

Individuals' rights in their Personal Information

23. **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 Data Protection Officer. These rights can be exercised either in writing (e.g. in an email) or orally.

24. Individual's rights: Please let Data Protection Officer know if anyone (either for themselves or on behalf of another person, such as their child):
    24.1 wants to know what information the School holds about them or their child;

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

    24.3 wants the School to delete any information;

    24.4 asks the School to correct or change information (unless this is a routine updating of information such as contact details);

    24.5 asks for personal information to be transferred to them or to another organisation;

    24.6 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 alumni events information; or

    24.7 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.

25. 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 School who is preparing a response to a request for information then you must make sure that you provide everything.

Requests for Personal Information (Subject Access Requests)

26. **The right to request Personal Information:** One of the most commonly exercised rights mentioned in paragraph above is the right to make a Subject Access Request. Under this right people are entitled to request a copy of the Personal Information which the School holds about them (or in some cases their child) and to certain supplemental information.

27. **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 Data Protection Officer know when you receive any such requests.

28. **If you receive a Subject Access Request**: 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.

29. **Disclosure**: When a Subject Access Request is made, the School must disclose all of that person's Personal Information to them which falls within the scope of the 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.

Breach

30. **Breach:** A breach of this policy may be treated as misconduct and could result in disciplinary action.

31. **Criminal offence:** A member of staff who deliberately or recklessly obtains or discloses Personal Information held by the School without proper authority could also be guilty of a criminal offence.

Author: Director of Finance,

Approved: Finance & General Purposes Committee

Reviewed: September 2026

Next Review Date: September 2027