

Data Protection Policy for Staff

Independent Day School for Boys and Girls

The Corporation of King's College School

King's College School, Wimbledon

King's College Junior School, Wimbledon

Wimbledon Common Preparatory School

June 2018

1 Introduction

- 1.1 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 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.
- 1.2 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 school and will ensure that the school operates successfully.
- 1.3 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.
- 1.4 The bursar is responsible for helping you to comply with the school's obligations. All queries concerning data protection matters should be raised with the bursar.

2 Application

- 2.1 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, peripatetic staff, coaches, work experience / placement students and volunteers.
- 2.2 This policy does not form part of your contract of employment and may be amended by the school at any time.

3 What information falls within the scope of this policy

- 3.1 Data protection concerns information about individuals.
- 3.2 Personal Data is data that relates to a living person who can be identified either from that data, or from the data and other information that is available.
- 3.3 Information as simple as someone's name and address is their Personal Data.
- 3.4 In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data.
- 3.5 Examples of places where Personal Data might be found are:
 - 3.5.1 on a computer database;
 - 3.5.2 in a file, such as a pupil report;
 - 3.5.3 a register or contract of employment;
 - 3.5.4 pupils' exercise books, coursework and mark books;
 - 3.5.5 health records; and
 - 3.5.6 email correspondence.
- 3.6 Examples of documents where Personal Data might be found are:
 - 3.6.1 a report about a child protection incident;
 - 3.6.2 a record about disciplinary action taken against a member of staff;

- 3.6.3 photographs of pupils;
 - 3.6.4 a tape recording of a job interview;
 - 3.6.5 contact details and other personal information held about pupils, parents and staff and their families;
 - 3.6.6 contact details of a member of the public who is enquiring about placing their child at the School;
 - 3.6.7 financial records of a parent;
 - 3.6.8 information on a pupil's performance; and
 - 3.6.9 an opinion about a parent or colleague in an email.
- 3.7 These are just examples - there may be many other things that you use and create that would be considered Personal Data.
- 3.8 You must be particularly careful when dealing with Personal Data which falls into any of the categories below:
- 3.8.1 information pertaining to an individual about a safeguarding matter;
 - 3.8.2 documents which contain all of a person's name, address and date of birth;
 - 3.8.3 information about serious or confidential medical conditions or reports of an accident;
 - 3.8.4 information about special educational needs specific to and identifiable to an individual;
 - 3.8.5 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) and information relating to actual or alleged criminal activity. This would include, for example, information about an alleged grievance or disciplinary matter;
 - 3.8.6 financial information (for example about parents and staff) including bank details and/or information indicating a person's wealth / debts/ salary.
 - 3.8.7 information about an individual's protected characteristics (race, ethnicity, sexual life and orientation);
 - 3.8.8 political opinions, religious beliefs or other beliefs of a similar nature, trade union membership;
 - 3.8.9 physical or mental health or conditions;
 - 3.8.10 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);
- 3.9 These categories are referred to as **Critical Personal Data** in this policy and in the Information Security Policy. If you have any questions about your processing of these categories of Personal Data please speak to the bursar.

4 Your obligations

4.1 Personal Data must be processed fairly, lawfully and transparently

4.1.1 What does this mean in practice?

- (a) "Processing" covers virtually everything that is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.
- (b) 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 the 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. Copies of the school's privacy notices can be obtained from the bursar or accessed on the school's website or Staff Handbook. You must familiarise yourself with the School's Pupil, Parent and Staff Privacy notices.

- (c) If you are using Personal Data in a way which you think an individual might think is unfair please speak to the bursar.
- (d) You must only process Personal Data for the following purposes:
 - (i) ensuring that the school provides a safe and secure environment;
 - (ii) providing pastoral care;
 - (iii) providing education and learning for our pupils;
 - (iv) providing additional activities for pupils and parents (for example activity clubs);
 - (v) protecting and promoting the school's interests and objectives (for example fundraising);
 - (vi) safeguarding and promoting the welfare of our pupils; and
 - (vii) to fulfil the school's contractual and other legal obligations.
- (e) 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, you must speak to the bursar. This is to make sure that the school has a lawful reason for using the Personal Data.
- (f) 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 bursar if you think that you may need to obtain consent. As a general guide, please speak to bursar before using Personal Data in a way that strikes you as unusual or more privacy intrusive or in a way in which an individual would not reasonably expect. For example, if a third party asks for information about a parent or pupil.
- (g) If you are not an employee of the school (for example if you are 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.

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

What does this mean in practice?

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 Guidance for Staff on the use of Photographs and Videos of Pupils for further information relating to the use of photographs and videos.

4.3 Personal Data held must be adequate and relevant for the purpose

What does this mean in practice?

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

4.4 You must not hold excessive or unnecessary Personal Data

What does this mean in practice?

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 religious belief if that Personal Data has some relevance, such as determining the dates that should be avoided for a school activity.

4.5 The Personal Data that you hold must be accurate

What does this mean in practice?

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 ask them to update their records through the parent portal.

4.6 You must not keep Personal Data longer than necessary

What does this mean in practice?

- (a) The school has a Records Retention Policy which sets out 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.
- (b) Please speak to the bursar if you require further guidance on the retention periods and secure deletion.

4.7 You must keep Personal Data secure

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

- (a) information security policy;
- (b) guidance for staff on the use of photographs and videos of pupils;
- (c) IT acceptable use policy for staff; and

- (d) information and records retention policy.

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

What does this mean in practice?

- (a) The school has safeguards in place for transfers outside of the EEA which relate to our routine activities. This would be relevant where, for example, the school needs to send pupil information to parents living overseas, or where you access your emails whilst on holiday outside of the EEA, or use Cloud based storage.
- (b) However, if you need to transfer personal data outside the EEA for less routine reasons please contact the bursar. For example, if you are arranging a school trip to a country outside the EEA.

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

5.1 Please read and comply with the following dos and don'ts:

- 5.1.1 **DO** share Personal Data on a need to know basis - think about why it is necessary to share data outside of the School - if in doubt - always ask your head of department.
- 5.1.2 **DO** encrypt emails which contain Critical School Personal Data described in paragraph 3.8 above. For example, encryption should be used when sending details of a safeguarding incident to social services.
- 5.1.3 **DO** make sure that you have permission from your head of department or the bursar to share Personal Data on the school website.
- 5.1.4 **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 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).
- 5.1.5 **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 asks 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.
- 5.1.6 **DO NOT** disclose Personal Data to the Police or the NHS without asking the Bursar, unless in your reasonable opinion it is an emergency and it is not possible to obtain the consent of the data subject.
- 5.1.7 **DO NOT** disclose Personal Data to contractors without permission from the bursar. This includes, for example, sharing Personal Data with a printing company used to prepare publications such as the school prospectus. The bursar will ensure that there is the appropriate contractual documents in place with the contractor.

6 Sharing Personal Data within the School

- 6.1 This section applies when Personal Data is shared within the school. It also applies when Personal Data is shared between schools in the Corporation.
- 6.2 Personal Data must only be shared within the school on a "need to know" basis.
- 6.3 Examples of sharing which are **likely** to comply with the Act:
- 6.3.1 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);
 - 6.3.2 informing an exam invigilator that a particular pupil suffers from panic attacks; and
 - 6.3.3 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).
- 6.4 Examples of sharing which are **unlikely** to comply with the Act:
- 6.4.1 the head being given access to all records kept by nurses working within the school (seniority does not necessarily mean a right of access);
 - 6.4.2 informing all staff that a pupil has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil); and
 - 6.4.3 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).
- 6.5 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 director of human resources.

7 Individuals' rights in their Personal Data

- 7.1 People have various rights in their information.
- 7.2 You must be able to recognise when someone is exercising their rights so that you can refer the matter to the bursar.
- (a) Please let the bursar know if anyone (either for themselves or on behalf of another person, such as their child):
 - (i) wants to know what information the school holds about them or their child;
 - (ii) asks to withdraw any consent that they have given to use their information or information about their child;
 - (iii) wants the school to delete any information;
 - (iv) asks the school to correct or change information (unless this is a routine updating of information such as contact details);

- (v) asks for electronic information which they provided to the school to be transferred back to them or to another organisation;
- (vi) 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
- (vii) 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.

8 Requests for Personal Data (Subject Access Requests)

- 8.1 One of the most commonly exercised rights mentioned in section 7 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.
- 8.2 Specifically, people are entitled to know:
 - 8.2.1 whether the school is holding Personal Data which relates to them or in some cases their child;
 - 8.2.2 what that information is i.e. to receive a copy of their Personal Data;
 - 8.2.3 the source of the Personal Data;
 - 8.2.4 how the school uses the Personal Data; and
 - 8.2.5 who the Personal Data has been disclosed to.
- 8.3 Subject access requests do not have to be labelled as such and do not even have to mention data protection. For example, an email that 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. If you receive a request for personal data, however it is phrased please follow the **subject access request protocol** appended to this policy.
- 8.4 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.
- 8.5 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 their 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.

9 Breach of this policy

- 9.1 Any breach of this policy will be taken seriously and may result in disciplinary action. In serious cases this could amount to gross misconduct and result in summary dismissal.

- 9.2 A member of staff who deliberately or recklessly discloses Personal Data held by the school without proper authority is guilty of a criminal offence.

Appendix I

Subject Access Request Protocol

Step ONE

If you receive any written request for release of personal information forward it immediately to the bursar and compliance officer. A request must be in writing but can be phrased very generally. It does not have to say it is a “subject access request”. If possible make it clear in your communication to the bursar and the compliance officer that you think this is a possible subject access request.

Step TWO

On receipt of a subject access request from staff member AMC or JVM will:

- Determine the scope of request and identify the departments concerned.
- Determine the dates that the data subject attended / worked at the school. If the data subject attended worked at the school before email for instance, it would not be necessary to conduct a search of the email archive.
- Clarify the specific areas of the the request and specify a response date.
- Confirm receipt of request.
- Diarise deadline for providing material (generally one calendar month from date of receipt) and diarise weekly reminders.

Departments and contact names	
HR	Tanya Allen
Finance	Jennie Macdougall
Admissions	Stephanie Dowling (SS) Suzie Richard (JS)
Teaching Staff	Deputy Head (pastoral) JS and SS Deputy Head (academic) JS and SS
Medical	Siobhan Besley
IT(email,	Ollie Knight / Database manager
Alumni and Development	Adriana Williams
Archives	Archives Manager
WCPS	Tracey Buck

Step THREE

AMC or JVM will issue an email to all departments affected by the request marked as high importance:

Title: **subject access request search**

We have been asked to provide information on [insert name] who attended the school between [insert dates]. Please can you search your hard copy and electronic database for information that we hold on this pupil [specify area of information required if possible] and update the bursar by [insert date prior to deadline].

Step FOUR

JVM /AMC remind departments on a weekly basis to provide data or confirm no data held. school's ability to meet the deadline to provide the data will also be reviewed weekly. If it is an extensive search the school may need more time to conduct the search. The data subject should be kept updated if there is a delay.

Step FIVE

AMC contacts the data subject and confirms the results of the search.

JVM

June 2018