CRANLEIGH
PREPARATORY SCHOOL

CRANLEIGH
EX CULTU ROBUR

DATA PROTECTION POLICY

1 Introduction

1.1 This policy is about your obligations under UK data protection legislation. Data protection is about ensuring the School remains compliant in the way it uses and stores information about a living person who can be identified either from that data, or from the data and other information that is available. This data/information is known as Personal Data.

1.2 Data protection legislation gives people various rights regarding their data, such as the right to be informed about how their data is being used, to have access to the Personal Data that the School holds on them, to have incorrect data updated, and to have data erased. (See section 7.)

1.3 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 that the School takes a pro-active and compliant approach to protecting Personal Data, overseen by the Senior Management Team and Governing Body.

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

1.5 The Data Protection Lead 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 Lead.

2 Application

2.1 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 / gap year / placement students and volunteers.

2.2 Employees only: this policy does not form part of your contract of employment and may be amended by the School at any time.

3 Scope of this policy

3.1 Personal Data is information that relates to a living person who can be identified either from that information alone, or from the information when combined with other information.

3.2 Information as simple as someone's name and address is their Personal Data.

3.3 In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data.

3.4 Examples of places where Personal Data might be found are:

3.4.1 on a computer database;

3.4.2 in a file, such as a pupil report;

3.4.3 a register or contract of employment;

3.4.4 pupils' exercise books, coursework and mark books;

3.4.5 health records; and

3.4.6 email correspondence.

3.5 Examples of documents where Personal Data might be found are:

3.5.1 a report about a child protection or safeguarding incident;

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

3.5.3 photographs and videos of pupils;

3.5.4 a record of a job application or interview;

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

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

3.5.7 financial records of a parent;

3.5.8 information on a pupil's performance; and

3.5.9 an opinion about a parent or colleague in an email.

3.6 These are just examples of a range of electronic and hardcopy datasets, held in a variety of formats - there may be many other things that you use and create that would be considered Personal Data.

3.7 **Critical School Personal Data**: The following categories are referred to as **Critical School Personal Data** in this policy and in the Information Security policy. There are stronger legal protections for this type of information and you must therefore be particularly careful when handling any Critical School Personal Data.

3.8 Critical School Personal Data which is information about:

3.8.1 safeguarding and/or child protection matters;

3.8.2 someone's special educational needs;

3.8.3 a serious allegation made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);

3.8.4 financial information (for example, a parent's bank details or a staff member's bank details and salary);

3.8.5 an individual's racial or ethnic origin;

3.8.6 an individual's political opinions;

3.8.7 an individual's religious or philosophical beliefs;

3.8.8 trade union membership;

3.8.9 an individual's physical or mental health. or condition. This includes information about the provision of healthcare which reveals information about their health status;

3.8.10 sex life or sexual orientation;

3.8.11 genetic information;

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

3.8.13 biometric information used for the purpose of uniquely identifying an individual (e.g. fingerprints used for controlling access to a building).

3.9 If you have any questions about your using of these categories of Critical School Personal Data please speak to the Data Protection Lead.

4 Your obligations under the Data Protection Act: Everyone responsible for using Personal Data must adhere to the core Data Protection Principles:

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 which is done in relation to Personal Data, including using, sharing (internally or externally), copying and storing it.

(b) 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 relation to their data, 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 provided in a document known as a privacy notice. Copies of the School's privacy notices can be obtained from the Data Protection Lead or accessed on the School's website. 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, or in a way that they might not expect, please speak to the Data Protection Lead.

(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 including safeguarding, child protection and

promoting the welfare of our pupils;

(iii) in relation to HR and staff matters;

(iv) providing education and learning for our pupils;

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

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

(vii) to fulfil the School's contractual and other legal obligations.

(e) **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 Data Protection Lead. This is to make sure that the School can lawfully use the Personal Data.

(f) **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 Data Protection Lead if you think that you may need to seek consent.

(g) 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 data in a way that has been expressly authorised by the School.

4.2 **You must only process Personal Data for specified, explicit and legitimate purposes.**

4.2.1 What does this mean in practice?

(a) 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).

(b) Please see the School's Code of Conduct and the Guidance for Staff on the use of Photographs and Videos for further information relating to the use of photographs and videos.

4.3 **Personal Data held must be adequate, relevant and limited to the specified purpose**

4.3.1 What does this mean in practice?

(a) 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 and when making a note of a disciplinary incident you must include all relevant details.

4.4 **You must not collect or use excessive or unnecessary Personal Data**

4.4.1 What does this mean in practice?

(a) You must limit the Personal Data that you collect or use to the minimum needed to meet your objectives. For example, you do not need to share with all staff that a pupil has a health condition, only those staff that need to know; or 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.

4.5 **The Personal Data that you hold must be accurate and kept up to date**

4.5.1 What does this mean in practice?

(a) 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 School's information management system has been updated.

(b) Where possible, do not retain copies of data/duplicate lists outside of the information management system. If you need to extract data, for example into Excel for a specific purpose, please delete the xsl.data (electronic and hard copy versions) as soon as possible.

4.6 **You must not keep Personal Data longer than necessary**

4.6.1 What does this this mean in practice?

(a) The School has an Information & Records Retention Policy in place, stating 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 or disposing of data and must check the poilicy before doing so.

(b) Please speak to the Data Protection Lead for guidance on retention periods and secure deletion/destruction of data.

4.7 **You must keep Personal Data secure**

4.7.1 This is a high-risk area of data protection for the School. You must ensure that data is handled in a way that ensures appropriate integrity, confidentiality and security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

4.7.2 Personal Data must be kept safe at all times. This includes paper and electronic information. This is a critical area of compliance, most data protection fines and compensation claims happen because of security breaches.

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

(a) Information Security Policy;

(b) Guidance for Staff on the use of Photographs and Videos;

(c) Security, CCTV and Pupil Safety Policy;

(d) IT Acceptable Use policy for staff; and

(e) Information and Records Retention Policy

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

4.8.1 What does this mean in practice?

(a) If you need to transfer personal data outside the UK please contact the Data Protection Lead. For example, if you are arranging a school trip to a country outside the UK.

4.9 **Accountability**

4.9.1 The School is responsible for and must be able to demonstrate its 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.

4.9.2 Before using Personal Data in a new way, or in a way that might present a risk to individuals if something went wrong (e.g. before implementing new software to store medical information) please speak to the Data Protection Lead

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

5.1 **Dos and Don'ts:** Please review the following dos and don'ts:

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

5.1.2 **DO** encrypt emails which contain Critical School Personal Data described in paragraph 3.7 above. For example, encryption must be used when sending details of a safeguarding incident to social services. Further information on encryption can be found in the Information Security policy.

5.1.3 **DO** make sure that you have permission from your line manager or the Director of Operations to share Personal Data on the School website or social media accounts.

5.1.4 **DO** check with your line manager or the Data Protection Lead before using an app or other software that has not been authorised by the School.

5.1.5 **DO** share Personal Data in accordance with the School's safeguarding and child protection policy. If you have any questions or concerns relating to safeguarding or child protection, you must contact the Designated Safeguarding Lead.

5.1.6 **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 Data Protection Lead 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).

5.1.7 **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 information, 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. Further information on blagging and phishing can be found in the information security policy.

5.1.8 **DO NOT** disclose Personal Data to the Police without permission from the Director of Operations (unless it is an emergency).

5.1.9 **DO NOT** disclose Personal Data to contractors or service providers without permission from the Director of Operations. This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil recruitment event or with an online app or website.

6 Accessing or sharing Personal Data within the School

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

6.2 **Need to Know Basis:** Personal Data must only be accessed or shared within the School on a "need to know" basis.

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

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 sharing Personal Data in accordance with the School's safeguarding and child protection policy;

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

6.3.4 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).

6.4 Examples which are **unlikely** to comply with data protection legislation:

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 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. Accessing records without good reason may result in disciplinary action and could, in fact, be a criminal offence (see paragraph 9.2 below);

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

6.4.4 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 **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 and child protection issues. If you have not received this training please contact the Personnel Department as a matter of urgency.

7 Individuals' Rights regarding their Personal Data

7.1 People have various rights regarding the personal data held about them, such as the right to:

- be informed about how their data is being used
- have access to their personal data (by making a Subject Access Request)
- have incorrect data amended/updated
- have data erased
- stop or restrict the processing of their data
- data portability (allowing the data subject to get and reuse data for different services)
- object to how data is processed in certain circumstances

7.2 You must be able to recognise when someone is exercising their rights so that you can refer the matter to the Data Protection Lead. These rights can be exercised either in writing (e.g. in an email) or orally.

(a) Please let the Data Protection Lead know if anyone (either for themselves or on behalf of another person, such as their child):

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

(ii) asks to withdraw any consent that they have given to use their Personal Data or Personal Data about their child;

(iii) wants the School to delete any Personal Data;

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

(v) asks for personal data to be transferred to them or to another organisation;

(vi) 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;

(vii) 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

(viii) wants the School to stop using a computer programme to make an important decision about them.

(b) 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.

8 Requests for Personal Data (Subject Access Requests)

8.1 **The right to request Personal Data:** 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 **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 let the Data Protection Lead know immediately on receiving any such requests.

8.3 **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. A subject access request must be forwarded to the Data Protection Lead and/or Director of Operations without delay.

8.4 **Disclosure:** 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 unprofessional comments or embarrassing information - so think carefully when writing file notes, letters and emails, avoiding subjective or defamatory comments, as they could be disclosed following a subject access request. However, this must not deter you from recording and passing on full and accurate information where this is appropriate to fulfil your professional duties, particularly in relation to safeguarding or child protection matters.

9 Breach

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

9.2 **Criminal Offence:** A member of staff who deliberately or recklessly obtains or discloses Personal Data held by the School (or facilitates 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 Data Protection Lead before doing this.