Data Protection Policy

COOMBE HOUSE
SCHOOL

Policy owner:	Mark Blackman	**Adoption Date:** November 2021
Approved by company	Mark Blackman	
Review cycle	Annual	
Last reviewed on:		
Next review due by:	November 2022	

Dorset Centre of Excellence

Contents

Introduction

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

2 The Company is ultimately responsible for how staff handle Personal Data.

3 **Lawful treatment of data**: 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 Company and will ensure that the Company operates successfully.

4 In addition to this policy, you must also read the following which are relevant to data protection:

4.1 the Company's privacy notices for staff, pupils and parents;

4.2 IT acceptable use policy for staff;

4.3 the information security policy; and

4.4 guidance for staff on the use of photographs and videos of pupils by the Company.

5 **Application:** This policy is aimed at all staff working in the Company (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, directors, contractors, agency staff, work experience / placement students and volunteers.

6 **Obligation:** You are obliged to comply with this policy when processing Personal Data on the Company's behalf. Any breach of this policy may result in disciplinary action.

7 **Queries:** The Data Protection Officer is responsible for helping you to comply with the Company'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

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

9 **Personal Data:** 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.

10 **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.

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

11.1 on a computer database;

11.2 in a file, such as a pupil report;

11.3 a register or contract of employment;

11.4 pupils' exercise books, coursework and mark books;

11.5 health records; and

11.6 email correspondence.

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

12.1 a report about a child protection incident;

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

12.3 photographs and videos of pupils;

12.4 a tape recording of a job interview;

12.5 contact details and other personal information held about pupils, parents and staff and their families;

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

12.7 financial records of a parent;

12.8 information on a pupil's performance; and

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

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

14 Categories of Critical Personal Data: The following categories are referred to as Critical Personal Data in this policy and in the information security policy. Critical School Personal Data is Information which concerns:

14.1 safeguarding or child protection matters;

14.2 serious or confidential medical conditions;

14.3 special educational needs;

14.4 financial information including parent and staff bank details;

14.5 an individual's racial or ethnic origin;

14.6 political opinions;

14.7 religious beliefs or other beliefs of a similar nature;

14.8 trade union membership;

14.9 someone's physical or mental health or condition;

14.10 sex life including sexual orientation;

14.11 actual or alleged criminal activity;

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

14.13 biometrics (for example if the Company uses a fingerprint scanner for allowing access to buildings); and

14.14 genetic information.

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

Your obligations

15 **Personal Data must be processed fairly, lawfully and transparently**

15.1 What does this mean in practice?

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

15.1.2 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).

15.2 This information is often provided in a document known as a privacy notice or a transparency notice. Copies of the Company's privacy notices can be accessed on the staff portal. You must familiarise yourself with the Company's Pupil, Parent and Staff Privacy notices.

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

16 **You must only process Personal Data for the following purposes:**

16.1 ensuring that the Company provides a safe and secure environment;

16.2 providing pastoral care;

16.3 providing education and learning for our pupils;

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

16.5 protecting and promoting the Company's interests and objectives (for example fundraising);

16.6 safeguarding and promoting the welfare of our pupils; and

16.7 to fulfil the Company's contractual and other legal obligations.

17 **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 Officer. This is to make sure that the Company has a lawful reason for using the Personal Data.

18 **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 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 Company (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 Company.

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

19.1 What does this mean in practice?

19.1.1 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 Company'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.

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

20.1 What does this mean in practice?

20.1.1 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.

21 **You must not hold excessive or unnecessary Personal Data.**

21.1 What does this mean in practice?

21.1.1 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 medical history if that Personal Data has some relevance, such as allowing the Company to care for the pupil and meet their medical needs.

22 **The Personal Data that you hold must be accurate.**

22.1 What does this mean in practice?

22.1.1 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 should update the Company's information management system.

23 **You must not keep Personal Data longer than necessary.**

23.1 What does this this mean in practice?

23.1.1 The Company 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.

23.1.2 Please speak to the Data Protection Officer for guidance on the retention

periods and secure deletion.

24 **You must keep Personal Data secure.**

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

24.1.1 information security policy;

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

24.1.3 IT acceptable use policy for staff; and

24.1.4 information and records retention policy.

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

25.1 What does this mean in practice?

25.1.1 The EEA is the EU member states plus Iceland, Liechtenstein and Norway.

25.1.2 If you need to transfer Personal Data outside the EEA please contact the HR and Operations Manager / Data Protection Officer. For example, if you are arranging a school trip to a country outside the EEA.

26 **Accountability**

26.1 The Company 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 Company - dos and don'ts

27 Please review the following dos and don'ts:

27.1 **DO** share Personal Data on a need-to-know basis - think about why it is necessary to share data outside of the Company - if in doubt - always ask your Data Protection Officer

27.2 **DO** encrypt emails which contain Critical Personal Data described in paragraph 14 above. For example, encryption should be used when sending details of a safeguarding incident to social services.

27.3 **DO** make sure that you have permission from your Data Protection Officer to share

Personal Data on the Company website.

27.4 **DO** check with your Data Protection Officer before using an app or other software that has not been authorised by the Company.

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

27.6 **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 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).

27.7 **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 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.

27.8 Further information on blagging and phishing can be found in the information security policy.

27.9 DO NOT disclose Personal Data to the Police without permission from the Data Protection Officer (unless it is an emergency).

27.10 **DO NOT** disclose Personal Data to contractors without permission from the Data Protection Officer. 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 Company

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

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

30 Examples which are likely to comply with data protection legislation:

30.1 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);

30.2 sharing Personal Data in accordance with the Company's Safeguarding Policy;

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

30.4 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).

31 Examples which are unlikely to comply with data protection legislation:

31.1 the Chief Operating Officer being given access to all records kept by nurses working within the Company (seniority does not necessarily mean a right of access);

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

31.3 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.

31.4 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).

32 **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.

Individuals' rights in their Personal Data

33 **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.

34 **Individual's rights:** Please let the HR and Operations Manager / Data Protection Officer know if anyone (either for themselves or on behalf of another person, such as their child):

34.1 wants to know what information the Company holds about them or their child;

34.2 asks to withdraw any consent that they have given to use their information or

information about their child;

34.3 wants the Company to delete any information;

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

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

34.6 wants the Company 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

34.7 objects to how the Company is using their information or wants the Company 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.

35 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 Company 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)

36 **The right to request Personal Data:** One of the most commonly exercised rights mentioned in paragraphs 33 to 34 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 Company holds about them (or in some cases their child) and to certain supplemental information.

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

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

39 **Disclosure:** When a subject access request is made, the Company 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.

Breach

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

41 **Criminal offence:** A member of staff who deliberately or recklessly obtains or discloses Personal Data held by the Company without proper authority is also guilty of a criminal offence.