Data protection policy for staff

SANCTON WOOD SCHOOL

September 2014

Andrew Gallie
Associate
E-mail: agallie@vwv.co.uk
DDI: 0117 314 5623
Reference: 4m540/0001

Veale Wasbrough Vizards

1 Introduction

1.1 **Background**: This policy concerns our obligations under the Data Protection Act 1998 (the **Act**). The purpose of the Act is to safeguard personal information. The Act covers issues such as data security, individuals' rights to access information about them and the use and disclosure of personal data.

1.2 **Application**: This policy is aimed at all staff including temporary staff, agency workers and volunteers. The policy explains our general approach to data protection and provides practical guidance which will help to ensure that we comply with the Act.

1.3 **Responsibility**: We are responsible for complying with the Act. The person with day-to-day responsibility for compliance with the Act is Richard Settle(the **Data Protection Officer**). All staff are responsible for complying with this policy.

1.4 **Relevance**: Data protection is important because it concerns an individual's right that their personal information is used in a manner that is fair and lawful. A breach of the Act could have serious consequences for us, the individual and staff.

2 What the Act covers

Information covered

2.1 The Act applies to personal information about individuals (called **Personal Data** in the Act). Virtually any information about someone is likely to be Personal Data. All of the following examples are likely to contain Personal Data and are therefore subject to the Act:

- Information about a child protection incident;
- A record about disciplinary action taken against a member of staff;
- A photograph of pupils;
- Contact details of a member of the public who is enquiring about placing their child with us; and
- Financial records of a parent.

2.2 If a record containing Personal Data is held on a computer then it will be covered by the Act. This is the case regardless of how the information is held. For example Personal Data stored in an email, in a spreadsheet or on a smartphone, are all caught by the Act.

2.3 Records held in paper files only are sometimes not covered by the Act although there are so many exceptions to this rule that best practice is to treat all information about individuals as covered by the Act whether it is held in a paper file or held on computer.

2.4 The Act applies to any **Processing** of Personal Data. Processing covers virtually anything done in relation to Personal Data. For example, using, disclosing, copying, even just storing, Personal Data are all covered by the Act.

Summary of the obligations under the Act

2.5 The main obligations under the Act relevant to staff are as follows:

- **Compliance with the eight data protection principles:** The Act contains eight data protection principles which set out how organisations should handle Personal Data. They cover issues such as what information needs to be given to the individual, information security and using individuals' Personal Data in a fair way.
- **Subject access requests:** The Act gives individuals a number of rights including a right to request a copy of the Personal Data we hold about them.
- **Sensitive Personal Data:** There are extra obligations in relation to Sensitive Personal Data, held by us. Sensitive Personal Data is information about an individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life and information relating to actual or alleged criminal activity.
- **Informing the individual:** We must tell the individual how their Personal Data will be used (unless it is obvious).

2.6 What these obligations mean in practice is explained below.

3 Data protection in practice

Purposes of Processing Personal Data

3.1 Personal Data should only be used for specific and legitimate purposes. In our case these are:

- ensuring that we provide a safe and secure environment;
- providing pastoral care;
- providing education and learning for children;
- providing additional activities for children and parents for example activity clubs;
- protecting and promoting our interests and objectives - this includes fundraising;
- safeguarding and promoting the welfare of children; and
- fulfilling our contractual and other legal obligations.

3.2 Staff must not Process Personal Data for any other purpose without the Data Protection Officer's permission.

3.3 Staff should not use Personal Data for any purpose that is incompatible with the purpose for which it was originally acquired without obtaining the Data Protection Officer's permission.

Disclosing Personal Data

3.4 Staff will frequently disclose Personal Data. For example staff may routinely discuss a child's activities and progress with parents. Similarly staff may discuss routine matters relating to the children with colleagues.

3.5 All of this is allowed by the Act but staff should not disclose Personal Data in circumstances which might be considered unusual, or where the Personal Data includes Sensitive Personal Data, without permission from the Data Protection Officer. Staff should always speak to the Data Protection Officer if in doubt about whether a disclosure of Personal Data is permissible.

3.6 We may share Personal Data with other organisations within the Minerva group for the purposes listed in paragraph 3.1 above. For example, we may share children's details for the purposes of a shared school trip.

3.7 Staff must not transfer Personal Data outside the European Economic Area (EEA) without the individual's permission unless we are satisfied that the individual's rights under the Act will be adequately protected and the transfer has been approved by the Data Protection Officer. This applies even if the transfer is to a pupil's parents or guardians living outside the EEA.

Handling Personal Data in general

3.8 We must Process Personal Data in a way that is fair to individuals. Compliance with this policy is likely to mean that the Processing is fair in most cases. However, the concept of fairness can be quite difficult to define and staff should inform the Data Protection Officer if they feel that any of the Processing of Personal Data appears to be unfair to any individual in any way even if the Processing appears to comply with the letter of this policy.

3.9 We must only keep Personal Data for as long as is reasonably necessary but staff should not delete records containing Personal Data without authorisation. Staff should consult with the Data Protection Officer for guidelines about how long to retain different categories of Personal Data.

3.10 Staff should ensure that Personal Data is complete and kept up-to-date. For example, if a parent notifies a member of staff that their contact details have changed, the member of staff should inform the Data Protection Officer so that our central record can be updated.

3.11 We must ensure that we have sufficient Persona Data. For example a teacher writing a report about a child should ensure that he/she has all the child's relevant records to hand.

3.12 We must not Process Personal Data in a way that is excessive or unnecessary. For example, should 8 children out of a possible of 20 attend a lunch event, the member of staff should only take records (such as information about allergies and parent contact details) of those 8.

Informing the Data Subject:

3.13 If we obtain Personal Data (whether from the individual or from a third party) we will need to explain to the individual what the Personal Data will be used for. This is sometimes called a **Privacy Notice.**

3.14 The Privacy Notice must explain what information will be collected, what it will be used for, which third parties (if any) it will be shared with and anything else which might be relevant.

3.15 Staff are not expected to routinely provide pupils, parents and others with a Privacy Notice as this should have already been provided.

3.16 Having said this, staff should inform the Data Protection Officer if they suspect that we are using Personal Data in a way which might not be covered by an existing Privacy Notice. This may be the case where, for example, staff are aware that we are collecting medical information about children without telling their parents what that information will be used for.

4 Data Security

4.1 A member of staff who deliberately or recklessly discloses Personal Data without proper authority is guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

Protecting Personal Data

4.2 Staff must do all that they can to ensure that Personal Data is not lost or damaged, or accessed or used without proper authority. In particular:

- Paper records which include confidential information shall be kept in a secure location and in a cabinet which is kept locked when unattended;
- Computers must be kept locked when not in use;
- We use a range of measures to protect Personal Data stored on computers, including file encryption, anti-virus and security software, user passwords, audit trails and back-up systems. These must be used in all cases. Passwords must be at least 8 characters in length, be difficult to guess and should be changed frequently;
- Staff must not remove Personal Data from our premises unless it is stored in an encrypted form on a password protected computer or memory device. Further information is available from the Data Protection Officer;
- Staff must not remove Sensitive Personal Data from our premises without permission from the Data Protection Officer;
- Staff must not use their own computers or their own email accounts when handling Personal Data. For example, they must not send work emails from us to their private email account;
- In addition, staff must not use their own devices to store or transport Personal Data and must instead only use devices issued by us. This applies to all devices such as USB sticks, CDs, and smartphones;
- Staff must not allow unauthorised access to our computers or computers containing Personal Data related to us. For example, staff should not allow their friends and family access to their work computers or work emails;

- Permission should be sought from the Data Protection Officer before publishing anything containing Personal Data (for example, uploading photographs of one of our trips to our website).
- Staff must not use or leave computers, memory portable electronic devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.

Sharing Personal Data with colleagues

4.3 Only staff with the appropriate authorisation may access any Personal Data. Personal Data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority or their relationship to the subject of the Personal Data, unless they need to know it for a legitimate purpose. Examples:

- Staff may disclose details of an assistant's allergy to bee stings to colleagues so that they will know how to respond, but more private health matters must be kept confidential; and
- Personal contact details for a member of staff (e.g. their home address and telephone number, and their private mobile telephone number and e-mail address) shall not be disclosed to parents, pupils or other members of staff unless the member of staff has given their permission.

Disposing of Personal Data

4.4 We should not keep any Personal Data for longer than is necessary and any record containing Personal Data which we no longer need to keep should be securely destroyed, in accordance with the appropriate retention period, unless the information contained in the record is not very sensitive.

4.5 When disposing of computer records containing Personal Data it is important to make sure that the record is permanently deleted. It is not sufficient just to move the file into the recycle bin. Specialist software should be used to permanently delete the computer record. Further information is available from the Head of IT.

5 Data protection related requests from individuals

5.1 Under the Act individuals have a number of rights. The most important of these is a right to request a copy of the Personal Data we hold about them (a **Subject Access Request**).

5.2 Should any staff receive a Subject Access Request then they must promptly forward it to the Data Protection Officer.

6 Further information

6.1 If staff have any questions about this policy or about data protection they should speak to the Data Protection Officer.

6.2 Similarly, all staff have an obligation to assist us and colleagues to comply with the Act. Therefore staff should also report any concerns, or any evidence of non-compliance, to the Data Protection Officer.

Authorised by	Richard Settle
Date	September 2014
Effective date of the policy	September 2014
Review date	On each anniversary of the effective date of the policy and immediately following any data protection related incident.
Circulation	To all staff (including temporary staff, volunteers and agency workers)

Sancton Wood School

Data protection policy for staff