

Southover Partnership Data Protection Policy



Date adopted	September 2014
Review date:	May 2024
Next Review	May 2025

Contents

Southover Partnership Data Protection Policy	1
Employee's Personal Data.....	2
Data Security.....	3
Data Breaches	3
Disclosure of Information	4

The school is fully committed to compliance with all legal requirements regarding data protection. The legislation applies to anyone processing personal data. It sets out principles which should be followed, and it also gives rights to those whose data is being processed.

To this end, the school endorses fully and adheres to the eight principles of data protection as follows:

- data must be processed fairly and lawfully
- data must only be obtained for specified and lawful purposes
- data must be adequate, relevant and not excessive
- data must be accurate and up to date
- data must not be kept for longer than necessary
- data must be processed in accordance with the “data subject’s” (the individual’s) rights
- data must be securely kept
- data must not be transferred to any other country without adequate protection in place

Employee's Personal Data

Throughout employment and for as long as is necessary after the termination of your employment, the school will need to process data about you. The kind of data that the school will process includes:

any references obtained during recruitment
details of terms of employment
payroll details
tax and national insurance information
details of job duties
details of health and sickness absence records
information about performance
details of any disciplinary investigations and proceedings
training records
emergency contact details
correspondence with the school and other information that you have given the school

The school believes that those records used are consistent with the employment relationship between the school and yourself, and with the data protection principles. The data the School holds will be for management and administrative use only, but the School may, from time to

time, need to disclose some data it holds about you to relevant third parties (e.g. where legally obliged to do so by HM Revenue & Customs or where requested to do so by yourself for the purpose of giving a reference).

In some cases, the School may hold sensitive data, as defined by the legislation, about you. For example, this could be information about health, racial or ethnic origin, criminal convictions, trade union membership, or religious beliefs. This information may be processed not only to meet the School's legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment, and to comply with equal opportunity legislation. Since the processing of this type of information could possibly cause concern or distress, you will be asked to give express consent, unless the school has a specific legal requirement to process such data.

Subject to the requirements of the legislation, you may inspect and/or have a copy, of information in your own personnel file and/or other specified personal data and, if necessary, require corrections or deletions should such records be faulty. If you wish to do so you should make a written request to your line Manager.

Data Security

You are responsible for ensuring that any personal data that you hold and/or process as part of your job role is stored securely. You should ensure that you are aware of any specific requirements to process and secure data in relation to your job role and function within the school.

You must ensure that personal data is not disclosed either orally or in writing, or via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party.

You should note that unauthorised disclosure may result in action under the disciplinary procedure, which may include dismissal for gross misconduct. Personal data should be kept in a locked filing cabinet, drawer, or safe. Electronic data should be coded, encrypted, or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

When travelling with a device containing personal data, you must ensure both the device and data is password protected. The device should be kept secure and where possible it should be locked away out of sight i.e., in the boot of a car. You should avoid travelling with hard copies of personal data where there is secure electronic storage available. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight i.e., in the boot of a car.

Data Breaches

Should you become aware that School data has been compromised or that there has been a "data breach" you should report this to your line manager and or the School's Data Protection Officer without delay.

You should ensure that throughout the course of your employment that you follow all rules in relation to data processing as above. Upon leaving the school you must ensure that all and any data in your possession is returned to the school. You must not retain any confidential information or School data in any format or medium.

Disclosure of Information

You must not directly or indirectly disclose to any unauthorised person any knowledge or information relating to school pupils, the School's business, or the business of any of the School's customers without first obtaining permission in writing from The School.

You must not use for your own purposes or profit or for any purposes other than those of the school, any information which you may acquire in relation to the school's and/or its customers' business.

The rules concerning disclosure of information apply both during and after your employment with the school.

Unauthorised access to Southover information, whether computerised or manual, may lead to disciplinary action being taken against you. In the case of computerised information "hacking" will be considered a dismissible offence.

At the time of leaving the school, for whatever reason, you are required to return all products, documentation or any other information related to the school and, if requested, confirm compliance of the same in writing.

In addition, the school reserves the right to request such information to be returned during any period of notice should it deem it possible that there could be a risk, intentional or otherwise, to Southover or commercially sensitive information being made available to other parties.