

## Forres Sandle Manor (Non-Academic) Policy

Policy Title	Data Protection
Policy Lead (Appointment (& Initials))	Bursar (CIJ)
Date of Last Review	January 2019
Date of Next Review	January 2021

### DATA PROTECTION

**The Data Protection Act 1998** is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or who has access to the personal records of employees, pupils and parents. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example employee personnel files that form part of a structured filing system.

The purpose of these rules is to ensure that you do not breach the Act, and that personal information is dealt with properly and securely. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from the Headmaster.

### **SCOPE**

Personal information or data is defined as any information that relates to a living individual who can be identified from that information, or other information held. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

FSM collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, and fee collection, as well as the many different types of research data used by FSM. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

You should be aware that, under the Act, you are personally accountable for your actions and can be held criminally liable if you knowingly, or recklessly, breach it. Any serious breach of data protection legislation will also be regarded as misconduct and will be dealt with under FSM's disciplinary procedures. If you access another employee's personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

## THE 8 PRINCIPLES

There are 8 data protection principles that are central to the Act. FSM and all its employees must comply with these principles at all times in its information-handling practices. In brief, the principles say that personal data must be:

- [1] Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data. The conditions are either that the employee has given consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the employee and consists of information relating to:
  - Race or ethnic origin.
  - Political opinions and trade union membership.
  - Religious or other beliefs.
  - Physical or mental health or condition.
  - Sexual life.
  - Criminal offences; both committed and alleged.
- [2] Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.
- [3] Adequate, relevant and not excessive. FSM will review personnel files on an annual basis to ensure they do not contain a backlog of out-of-date information and to check there is a sound business reason requiring information to continue to be held.
- [4] Accurate and kept up-to-date. If your personal information changes, for example you change address, you must inform the Bursary as soon as practicable so that FSM's records can be updated. FSM cannot be held responsible for any errors unless you have notified the relevant change.
- [5] Not kept for longer than is necessary. FSM will keep personnel files for no longer than six years after termination of employment. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which FSM decides it does not need to hold for a period of time will be destroyed after one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.
- [6] Processed in accordance with the rights of employees under the Act.
- [7] Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Personnel files are confidential and are stored in locked filing cabinets within locked offices. Only authorised employees have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on discs, memory sticks, portable hard drives or other removable storage media will be kept in locked filing cabinets or locked drawers when not in use by authorised employees. Data held on computer will be stored confidentially by means of password protection, encryption or coding, and again only authorised employees have access to that data. FSM has network backup procedures to ensure that data on computer cannot be accidentally lost or

destroyed.

- [8] Not transferred to a country or territory outside the European Economic Area (EEA) unless that country ensures an adequate level of protection for the processing of personal data.

## **RESPONSIBILITIES**

FSM must:

- Manage and process personal data properly.
- Protect the individuals' right to privacy.
- Provide an individual with access to all personal data held on them.
- Ensure that personal information cannot be accessed by a third party, who may wish to manipulate or radicalise, as per PREVENT guidelines.

As Data Controllers, FSM will notify the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website.

FSM will inform data subjects of why they need their personal information, how they will use it, and with whom it will be shared. The quality and accuracy of the information held will be checked regularly. Procedures are in place to ensure that information is not held longer than necessary, and that records are disposed of when no longer required. Personal information is only shared when it is necessary and legally appropriate to do so.

## **CONSENT TO PERSONAL INFORMATION BEING HELD**

FSM holds personal data about all employees. By signing your contract of employment, you have consented to that data being managed and processed by FSM. Agreement to FSM processing your personal data is a condition of your employment. FSM also holds limited sensitive personal data about its employees and, by signing your contract of employment, you give your explicit consent to FSM holding and processing that data (for example sickness absence records, health needs and equal opportunities monitoring data).

## **RIGHTS TO ACCESS PERSONAL INFORMATION**

You have the right, on request, to receive a copy of the personal information that FSM holds about you, including your personnel file, and to demand that any inaccurate data be corrected or removed. You also have the right on request to:

- Be told by FSM whether and for what purpose personal data about you is being processed.
- Be given a description of the data and the recipients to whom it may be disclosed.
- Have communicated in an intelligible form the personal data concerned, and any information available as to the source of the data.
- Be informed of the logic involved in computerised decision-making.

Upon request, FSM will provide you with a statement regarding the personal data held

about you. It will state all the types of personal data FSM holds and processes about you and the reasons for which they are processed. If you wish to access a copy of any personal data being held about you, you must make a written request to the Bursar.

## **OBLIGATIONS IN RELATION TO PERSONAL INFORMATION**

FSM employees must comply with the following guidelines at all times:

- Do not disclose confidential personal information to anyone except the data subject. In particular, it should not be given to someone from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this.
- Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone
- If you receive a request for personal information about another employee, you should forward this to the Headmaster or the Bursar who are responsible for dealing with such requests.
- Ensure any personal data you hold is kept securely, either in a locked filing cabinet or, if computerised, it is password protected.
- Remember that compliance with the Act is your personal responsibility. If you have any questions or concerns about the interpretation of these rules, please contact the Bursar immediately.