Forres Sandle Manor (Non-Academic) Policy

Policy Title	**Code of Practice on Handling Personal Information**
Policy Lead (Appointment (& Initials))	**Bursar (CIJ)**
Date of Last Review	**June 2018**
Date of Next Review	**June 2021**

CODE OF PRACTICE ON HANDLING PERSONAL INFORMATION

OVERVIEW

This Code of Practice concerns the collection, holding and disclosure of **personal** data relating to individuals.

The holding, processing or disclosure of information on individuals which you may handle in the course of your duties is subject to the General Data Protection Regulations (GDPR) (May 2018). It is FSM Policy for all members of staff comply with the Act and this Code of Practice.

The Code is guidance to FSM staff who collect or have access to personal data and information held by any method. It is not a substitute for any statutory requirements contained in the GDPR or any of the conditions in FSM's Privacy Policy. In any case of conflict, the statutory requirements and conditions take precedence over the Code.

Personal Data. Personal data is ***any*** data relating to an identified individual (the data subject) or to an individual who may be identifiable from that personal data if merged with other data. This includes personal data held on computer files or in manual records or in other forms such as USB sticks, external hard drives and personal computers or tablets.

COLLECTION OF PERSONAL DATA

FSM will normally collect personal data only for the purposes set out below, unless provided voluntarily by the data subject:

- Employees. Personal data on employees (past, present, and prospective candidates) required by law to be held by FSM as the employer and also as a condition of FSM's participation in pension arrangements. The term *employee* is to be construed widely in this case, to include contractors, consultants, part-time staff, and visiting and retired employees still engaged in activities at FSM.

- Pupils. Personal data on prospective pupils, current pupils, former pupils (all for administrative, pastoral and welfare purposes), and pupils' progress while at FSM including academic records.

- Others. Where their relationship with FSM warrants collection, including commercial relationships with suppliers of goods and services.

Fair & Lawful Processes.

- FSM will ***collect*** personal data both fairly and lawfully, and only when relevant to the specific and lawful purposes for which it is required. In all cases the personal data collected should be sufficient for the purposes for which it is collected and never excessive.

- FSM will ***hold*** personal data both fairly and lawfully. Personal data should be held only when relevant to the specific and lawful purposes for which it is required. In all cases, the personal data held should be no more than is sufficient for the purposes for which it is being held.

Confidentiality. All personal data is to be held securely and in confidence, subject to the disclosure provisions set out in this Code. All individuals having access to such personal data, whether employees or pupils or in some other capacity, must treat as confidential all information of a private nature about an individual and not communicate it to others except as provided for under this Code.

Relevancy, Accuracy and Disposal. Every effort is to be made to ensure that personal data held is relevant and accurate and, where appropriate, kept up to date. Once personal data is no longer needed by FSM it is not to be retained. Personal data that is surplus to FSM's needs is to be destroyed without jeopardising its confidentiality.

DISCLOSURE OF PERSONAL INFORMATION

Personal data may be disclosed only in line with the provisions of this Code. Personal data held for a declared purpose must not be used or disclosed in any manner that is inconsistent with that purpose.

The General Data Protection Regulations (GDPR) (May 18) gives the data subject the right to request copies of documents and records containing personal data about themselves.

Not all personal data held will be disclosed by FSM in response to a request from the data subject. FSM is obliged to consider whether it should disclose information:

- where disclosure would simultaneously disclose personal data about another person (unless that person consents to the disclosure)

- where the personal data was supplied in the expectation that the data subject would not see it (unless the supplier of the personal data consents to the disclosure)

FSM employees and visiting staff have the right of access to the personal data of others only in so far as their responsibilities and duties require.

Personal data not already in the public domain will not normally be communicated to those requesting it from outside FSM except where it is required by law.

FSM will take reasonable steps to advise data subjects of the purposes for which it will use the personal data held about them.

PRACTICAL GUIDANCE FOR STAFF

Do Not:

- process personal data unless you are sure that you, your department or FSM has obtained the consent of the individual concerned or that it is necessary to process the personal data in support of a contract with the person, or to meet a legal obligation.

- disclose any information (including giving references) about an individual to an external organisation without first checking that the individual consents to such disclosure, or, in the case of the police, checking with the Head or Bursar.

- write any comment about any individual that is unfair or untrue and that you would not be able to defend if challenged. You must assume that anything that you write about a person could be seen by that person.

Be vigilant if you are working off-site using personal data such as individualised medical or passport data, reference requests or exam results. Strict security measures must be applied to the transport and storage of all such data.

Ensure that all personal data is kept secure, not only from unauthorised access but from fire and other hazards.

Use the School Office shredder to dispose of any documents containing personal data.

Apply password protection to computers, screensavers, documents and portable drives (including all USB sticks containing personal data). All portable media is to have BitLocker encryption software installed, obtainable from the IT staff. Where possible keep office doors locked and adopt a ***clear desk policy*** for all personal data when you are absent.

Wherever possible only send ‘clean’ emails and avoid forwarding emails which include previous conversations, despite the attraction and logic of an audit trail.

If you are sending out data to someone other than staff, check that it does not include personal data of another person.

Only record and retain personal data that is necessary.

When on trips or sports fixtures, do not leave any personal data at the venue or on the minibus. Personal data is anything about a person/pupil other than their name (medical details for example).

Be wary of screen-shots when copying data to someone else as these may include other people’s data – including exam results.

When you process personal data you must ensure that it is accurate, relevant and not excessive in relation to your needs.

Information concerning individuals gathered in the course of your duties must not be communicated to other persons or bodies unless required to do so by law, or for the proper purposes of FSM business or with the consent of the individual concerned, and any disclosures of information must be consistent with this Code of Practice.

It is the responsibility of all members of FSM staff to ensure:

- appropriate measures are taken to prevent personal information (in whatever format) from being accidentally divulged to unauthorised persons, and that appropriate care is taken in disposing of printed information containing personal information

- within your work area, the current general guidance on handling personal information is followed, along with any specific additional measures that may apply

Staff who are data holders (this includes all HODs, every form teacher and all key administrative posts) may hold personal data only in accordance with FSM’s data policies. Data holders should make appropriate arrangements for security and access to their data whenever they are away from FSM, and are responsible for anticipating both security and access considerations in the event of emergencies such as power/utility failures, computer network failure, fire, flood or occupation of the work area by others not entitled to access the personal data.

You are not permitted to remove from FSM any personal data with the intention of processing this data elsewhere, unless such use is recognised and authorised, and is fully protected in all senses. Transporting data is not to compromise normal FSM standards of information security.

FSM will support any employee who faces court proceedings for alleged breaches of data protection law, if that employee has acted in a reasonable manner, and not in breach of this Code of Practice on Handling Personal Information.