

JAMES HOPE



COLLEGE

DATA PROTECTION

The General Data Protection Policy (GDPR)

The Data Protection Policy is to protect the rights and privacy of individuals, and to ensure that data about them are not processed without their knowledge and are processed with their consent wherever possible. The policy covers personal data relating to living individuals and defines a category of sensitive personal data which are subject to more stringent conditions on their processing than other personal data. The College is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

1. Scope of the policy

1.1 The Data Protection Policy applies to electronic and paper records held in structured filing systems containing personal data, meaning data which relates to living individuals who can be identified from the data. 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. The College collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the College.

2. Responsibilities

2.1 Data Protection means that the College must:

- Manage and process personal data properly
- Protect the individual's rights to privacy
- Provide an individual with access to all personal information held on them

2.2 The College's SLT is responsible for drawing up guidance on good data protection practice and promoting compliance with this guidance through advising staff on the creation, maintenance, storage and retention of their records which contain personal information.

2.5 Every member of staff that holds information about identifiable living individuals must comply with data protection in managing that information.

3. The Principles

3.1 James Hope College shall so far as be reasonably practicable comply with the Data Protection Principles (the Principles) GDPR to ensure all data is:

- fairly and lawfully processed
- processed for a lawful purpose
- adequate, relevant and not excessive
- accurate and up to date
- not kept for longer than necessary
- processed in accordance with data subject's rights
- secure
- not transferred to other countries without adequate protection

4. What is "Data"?

4.1 Data means:

- all personnel data kept or processed by computer
- all paper records kept in a structured file e.g. "Course Records" with a Named Index. A simple list of individuals prepared for a routine function, but not then stored in a way in which an individual can be readily identified, would not constitute a record. It does not apply to miscellaneous collections of paper about individuals, even if the collections are assembled in a file with the individual's name, and that file is kept in date order, with no means of readily identifying specific information except by looking at every document.

5. Personal Data

5.1 Personal data covers both facts and opinions about an individual. It includes information necessary for employment, such as the member of staff's name and address and details for payment of salary, and details regarding a student's record of achievement and progress at the college. Further details are at Annex A.

6. Processing of Personal Data

6.1 A member of staff's consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data and is not

otherwise exempt will remain confidential and will only be disclosed to third parties with the consent of the member of staff concerned.

7. Sensitive Personal Data

7.1 James Hope College may, from time to time, be required to process sensitive personal data regarding a member of staff. Sensitive personal data includes medical information and data relating to religion, race, trade union membership and criminal records and proceedings. Where sensitive personal data is processed by James Hope College, the explicit consent of the member of staff will generally be required in writing.

8. Rights of Access to Information

8.1 All staff have a right of access to information held by James Hope College. Any member of staff wishing to access their personal data should put their request in writing to the Principal. James Hope College will endeavour to respond to any such written requests as soon as is reasonably practicable, and in any event within 30 days for access to records, and 21 days to provide a reply to an access to information request. The information will be imparted to the member of staff as soon as is reasonably possible after it has come to the College's attention, within 30 days.

8.2 Students should have the right to inspect the information held about them. Current guidance is as follows:

- applications by parents of students or by students themselves asking to see if personal data is held about them on computer should be dealt with informally and immediately
- students can make requests to see information held on them. The principal will judge whether the student understands the nature of the request; if this is deemed to be the case, then the Principal will reply to the student
- parents or guardians should only make requests on behalf of their children if that request is in the interests of the child and not their own interests. A reply will be given to a request made on the child's behalf by a parent or guardian only if the Principal is satisfied that the child has authorised the request

9. Exemptions

9.1 Certain data is exempted from the from the above and that includes the following:

- the prevention or detection of crime
- the assessment of any tax or duty

- where the processing is necessary to exercise a right or obligation conferred or imposed by law upon James Hope College

9.2 The above are examples only of some of the exemptions. Any further information on exemptions should be sought from the Principal.

10. Accuracy

10.1 James Hope College will endeavour to ensure that all personal data held in relation to members of staff is accurate. Members of staff must notify the Principal via the College office of any changes to information held about them. A member of staff has the right to request that inaccurate information about them is erased.

11. Enforcement

11.1 If a member of the staff believes that James Hope College has not complied with this Policy, then he/she should utilise the College's Grievance Procedures and should also notify the Principal.

12. Security

12.1 Those responsible for handling data should apply comprehensive security procedures appropriate to their duties. These include:

- data should be kept locked in filing cabinets when not in use, unless the office is inaccessible to others
- offices should be kept locked when unoccupied. All those with access to offices, or to the files if appropriate, should be aware of these rules
- data information should not be left unattended outside the normal place of work
- any copies of data should be treated in the same manner
- a regular programme of "weeding" should be conducted to ensure that data which is no longer required is destroyed;

DATA PROTECTION OFFICER: (DPO)

Responsibility

To facilitate data protection compliance
Monitor compliance with the DGPR

All questions and issues regarding data protection compliance should be directed to the DPO.

Ruth Swart
Mobile: +234 7015349257
E-Mail: ruth.swart@jameshopecollege.edu.ng

Annex A

PERSONAL DATA

1. James Hope College retains personal files on all members of staff and students. Data used by the Bursary for processing wages and salaries are held on computer. Files contain personal information, including:

Information given by the Employee

- information given on job application forms or in CV's
- letters sent to the College as part of a job application
- other correspondence between the employee and the College
- data necessary for the employee's work, including but not limited to DCSF information, driving licence details, etc.
- next of kin details

Information produced or obtained by the College in the normal course of employment

- references from previous employers or educational establishments
- reports from DCSF under the Protection of Children and similar Acts
- Disclosure from the Criminal Records Bureau in accordance with the Code of Practice
- appraisal reports, disciplinary and grievance procedures, in accordance with the appropriate policies
- personal information necessary for the payment of wages and salaries, income tax and pensions contributions

Information produced by the College on behalf of the Employee

- references requested by and sent to other organisations such as, but not limited to, potential employers, Building Societies, etc.

Information produced or obtained by the College in the normal course regarding students

- previous college reports
- copies of references from previous colleges
- correspondence with parents
- examination results
- parents' addresses, contact numbers, etc