Data Protection Policy at Gibraltar College

2019/20

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
L ABECASIS	
Date of next review	January 2021

Aims and Objectives

This Data Protection policy is designed to ensure that Gibraltar College is both aware of and adheres to the 8 principles of data protection, namely that data:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Be processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the EEA, unless that country or territory also ensures an adequate level of protection

TO WHAT TYPES OF DATA DOES THE POLICY APPLY

This Data Protection Policy covers all digital and manual data processing relating to students and others. It not only includes personal information about individuals, but also data relevant to all matters relating to the individual's stay at the College. It therefore includes, for example, student records, emails relating to identifiable individuals, staff issues as well as curriculum team meeting minutes, student and staff references. In other words, data is not only that dealing with students but also that relating to the staff.

WHO IS RESPONSIBLE FOR DATA PROTECTION

This policy applies to any individual either studying or working at the College known as the 'Data Subject'.

Administrative & teaching staff at the College who will process the data will be known as 'Data Processors'.

The College Principal will be known as the 'Data Controller'. The College holds data and the Data Controller is ultimately responsible for implementation of the law. The data controller will be responsible for providing advice, guidance and direction on data protection issues within the College.

The College will deal directly with parents/legal guardians in respect of students under the age of 18.

The College will deal directly with students who are 18 or over. However, in the case of full-time students living with their parents, consent includes communication with parents or legal guardians. Under certain circumstances such as discipline problems, the College may contact parents if this is deemed beneficial for the student. If the student expressly requests in writing for parents not to be contacted, then the College is duty bound to oblige.

For staff, although much falls partly under the auspices of other Government departments, it is understood that employees will abide by the relevant Act. Any failure to follow the policy can therefore result in an outcome as prescribed by the law in conjunction with the relevant Government department. It must be understood that breaching the Act is in effect a criminal offence.

Any data subject who considers that the policy has not been adhered to, should raise the matter with the data controller initially. If the matter is not resolved it should be raised as a formal grievance.

Responsibilities of Staff and Students

All members of staff and students are responsible for:

- Checking that any information provided is accurate and up to date
- Informing the College of any changes to or errors in information, which they have provided, e.g. changes of address, contact numbers etc. They must ensure that changes are notified to the relevant tutor, teacher or member of the Student Services team.
- The College cannot be held responsible for any such errors unless the staff member or student has informed the College of them.

If and when, as part of their responsibilities, staff collect information from other sources, (e.g. about students' course work, references, work placement reports, references to other academic institutions, or details of personal circumstances), they must comply with the relevant College policy & guidelines

Data Security

All members of staff are responsible for ensuring that:

- Any personal data held is kept securely, for example
    - In a locked room, locked filing cabinet or locked drawer
    - On a PC, laptop or other device, it is password protected.
- Papers containing personal information are shredded before disposal
- Databases are closed and workstations securely locked when leaving the computer

This applies too to any data held, in any form, outside the College, i.e. at home.

Personal information must not be disclosed in any form or manner, accidentally or otherwise to any unauthorised third party.

If an approach for data is made by an external third party, the matter must be reported to the Data Controller immediately.

Rights to Access Information

All members of staff and students of the College have the right to access their personal data. Any person who wishes to exercise this right should contact the Data Controller, i.e. the Principal.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing to the Data Controller. The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 28 days.

Subject Consent

The College can only process personal data with the consent of the individual. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course. In some cases, if the data is sensitive, express consent must be obtained. This may include information about previous criminal convictions and information about disabilities.

Processing Sensitive Information

Sometimes it is necessary to process sensitive information about a person. This could be in the form of criminal convictions etc. This may be to ensure the College is a safe place for everyone, or to comply with other College policies, such as equal opportunities.

The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or conditions such as asthma, diabetes or disabilities. The College will only use the information for the protection of the health and safety of the individual, but will need consent to process this information, for example in the event of a medical emergency.

Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, students will be asked to give express consent for the College to do this. An offer of a place in a course may be withdrawn if an individual refuses to consent to this without good reason.

Examination Marks

Students will be provided with information about their marks for both coursework and examinations. This is within the provisions of the Ordinance relating to the release of data.

In any case, Awarding Bodies regulate this aspect too; in simple terms, examination results will only be given to the student unless s/he provides written authorisation for another person to collect the result.

Retention of Data

Data on students held in physical form such as files, examination results, application forms, coursework, etc is held on College premises by designated officers who are responsible for ensuring it is kept securely. Data is usually held indefinitely but may be destroyed after 6 years.

Data on students held in digital form such as attendance records, personal information, etc can only be accessed by staff members who must not disclose information unless required for normal academic and pastoral purposes.

Management of IT systems is the responsibility of the Gibraltar government's Information Technology & Logistics department. As such, they are responsible for the maintenance, storage and back up of servers on which all staff and student data is held.