Cambridge Ruskin International College (CRIC)
CPR M2: Data Protection
Version 1.16

1 Introduction

The regulations set out in this document are set down by QaSO compliance frameworks and, where appropriate, on the data protection and privacy criteria of the Navitas UK policy and compliance regulations to students and associated personnel of each College.

2 Students

2.1 Applicants and students (inclusive of alumni) are entitled to protection of their privacy, as are staff and others who might have dealings with CRIC. Privacy considerations normally apply to a great deal of information that the College may hold about students that may include a mix of personal data (address, age, enrolment status, etc.), academic progress (examination results, evaluation and assessment and academic standing) and personal welfare (family matters, medical matters, financial matters and so on).

2.2 College staff may require access at times to personal information about students. To the extent that the information is private, the College will restrict access to those staff that need the information in order to carry out their responsibilities in the personal and/or academic interests of students.

2.3 the College will not disclose personal information about students to other students, to people outside of the College (other than in accordance with any legal or academic obligations and the Partner University 'Processing and Controller Parties' as per the *RAA*) or to staff who have no need of access to the information unless students advise the College in writing, that they have given permission.

2.4 For students 18 years of age and over, the College does not release any information it holds about those individuals, including the address, or results, even to parents or close relatives, without permission.

2.5 Students who are under 18 years at the time of their enrolment are considered minors, and the conditions involving release of requested information to parents or nominated guardians is somewhat different, see CPR M1.

3 Staff, associates/affiliates and academic teaching staff

3.1 All staff, associates/affiliates and academic teaching staff are entitled to protection of their privacy. Privacy considerations normally apply to some information that the College may hold about its staff and academic teaching staff and may include a mix of personal data (address, qualifications, performance indicators, emergency contact details inclusive of family members, medical details and financial data).

3.2 CRIC staff in a line management role may require access at times to personal information about staff and academic teaching staff to ensure that performance management processes are effective and that they have access to emergency contact information in the case of a crisis. To the extent that the information is private, the College will restrict access to those staff who may need the information in order to carry out their responsibilities in the business and operational interests of the College and Navitas UK except where they conflict with any UK or European legislation.

3.3 the College undertakes not to disclose personal information about its staff and its associates/affiliates, to people outside the College (other than in accordance with any legal or commercial obligations as determined by Navitas UK) or to staff who have no need of access to the information (inclusive of consultants/contractors), unless staff and associates/affiliates advise the College in writing, that they have given permission.

4 Obligations

There are some exceptions to the general application of this policy, some of which are obligations imposed by law on the College. This information is governed by the general policy outlined in this document.

5 General policy

5.1 Definition

5.1.1 Personal Data

Information about living, identifiable individuals that is either held in a form in which it can be or is being processed automatically (this would in the main be on computer) or within a structured manual filing system. Statements of fact and expressions of opinion about an individual data subject are personal.

5.1.2 Data Protection Act (1998)

All staff in the College will comply with the Data Protection Principles which are set out in the Data Protection Act 1998. In summary these state that personal data shall:

i. Be obtained and processed lawfully and shall not be processed unless certain conditions are met.
ii. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
iii. Be adequate, relevant and not excessive for those purposes.
iv. Be accurate and kept up to date.
v. Not be kept for longer than is necessary for that purpose.
vi. Be processed in accordance with the data subject's rights.
vii. Be kept safe from unauthorised access, accidental loss or destruction.
viii. Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for data.

5.2 Employee obligations

5.2.1 All members of staff who record and/or process personal data in any form must ensure that they are working within the requirements of the 1998 Act, that they comply at all times with the Data Protection Principles (section 1b) and with the institutional regulations and procedures set out in this document and in any supplementary procedures which may be introduced from time to time.

5.2.2 Whilst the 1998 Act places certain responsibilities on the College, individual members of staff who control the contents of and/or process personal data are personally responsible for complying with the 1998 Act.

5.2.3 Breach of the 1998 Act may constitute a criminal offence for the individual as well as the College. A breach of the 1998 Act and/or a breach of the College's policy, regulations or procedures on data protection, may also be regarded as a disciplinary matter by the College.

5.2.4 All staff and associate/affiliates are responsible for:

i. Ensuring that any information they provide to the College in connection with their employment is accurate and up to date, and informing the College Director/Principal of any changes to information, which they have provided e.g. change of address.
ii. Checking the information that the College will send out from time to time, giving details of information kept and processed about them or about students in their department and returning it to the sender.

5.2.5 All staff and associates/affiliates are responsible for ensuring that:

i. Any personal data which they hold is kept securely.
ii. Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party, except with the permission of the individual.
iii. It is a condition of employment that employees will abide by the rules and policies made by the College.
iv. Any failure to follow that policy may therefore result in disciplinary proceedings. Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the Executive Leadership Team (ELT) or the College Director/Principal. If the matter is not resolved it should be raised as a formal grievance.

5.3 Student, staff and associate/affiliate obligations

Students and staff must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes to their personal data, for example of address, name, next of kin, are notified to the College.

5.4 Notification of data held and processed

All staff, students and other persons are entitled to:

i. Know what information the College holds and processes about them and why.
ii. Know how to gain observation access to it through the approved and appropriate processes and channels.
iii. Know how to keep it up-to-date.
iv. Know what the College is doing to comply with its obligations under the 1998 Act.

5.5 Equal opportunity

5.5.1 Some jobs will bring applicants into contact with young people under the age of 18. The College has a duty under enactments to ensure that staff are suitable for the job, and students for the courses, offered. The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use the College's facilities do not pose a threat or danger to other users. All members of staff who come into contact with students must have Disclosure and Barring Services clearance - this also pertains to academic teaching staff.

5.5.2 Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This is to ensure the College is a safe place for everyone, or to monitor other College policies.

5.6 The role of the College Management Team (CMT)

The role of the CMT is to examine inadequate data protection practices and make recommendations for their alteration to the Executive Leadership Team for NVT UK. The College Team also has a responsibility to develop procedures and guidelines within the College for compliance with the Data Protection Act 1998.

5.6.1 The role of the Executive Leadership Team (ELT) of Navitas UK

The ELT must examine the operational UK data protection practices and policy and ratify, where appropriate, recommendation. The Group also has a responsibility to develop procedures and guidelines within the UK structure for compliance with the Data Protection Act 1998.

5.6.2 The Navitas Executive Board of Directors retain the ultimate legal responsibility for Data Protection across the worldwide Group.

5.7 Responsibility for implementing data protection and privacy policy

The protection of data is a College policy priority and responsibility for implementing it rests with the College Director/Principal.

The policy will be disseminated to staff, and incorporated in relevant publications and discussed at induction programmes for staff and orientation programmes for students.

<ends>