DATA PRIVACY POLICY

Overview

The College needs to keep certain information about its employees, students, and other users to allow it to monitor performance, achievements, health & safety, safeguarding and human resource issues such as pay, pension information and sickness levels.

It is also necessary to process this information so that staff can be recruited and paid, reporting to HMRC and pension agencies is accurate and timely, courses can be organised, and legal obligations to funding bodies and other Government departments complied with.

The Data Privacy Policy outlines what employees, student and other stakeholders can expect from the College and there are supporting procedures for some of the areas included in this policy.

The Data Privacy Policy includes the College's policy on Privacy By Design and Privacy Impact Assessments.

Definitions:

For the avoidance of doubt, the College is the "Data Controller" and its employees, suppliers, contractors and students are the "Data Subjects".

A "Data Processor" is any party, be they internal or external to the College that processes the data on behalf of the college. For example, data is taken from the student records and a process run on that data to enable reporting to the Department of Education on student numbers.

The College's designated "Data Protection Officer" is the ***Finance Director.***

Personal information and data are deemed to have the exact same meaning and relate to personal facts associated with a living individual.

Legal Definition and Requirements:

To comply with the law, personal information must be collected and used fairly, stored safely, and not disclosed to any other person or organisation unlawfully. To do this, the college must comply with the General Data Protection Regulation which is set to replace the Data Protection Act 1998. The College's General Data Protection Policy details the College's approach to Data Protection.

Notification of Data Held and Processed

All staff, students, and other persons about which the College legitimately holds data are entitled to:

- know what information the College holds and processes about them and why
- know how to gain access to such data
- know how to keep such data up to date and request corrections where appropriate
- know what the College is doing to comply with its obligations under the General Data Protection Regulation
- know that they can request that information associated with them is removed from college systems or anonymized. Such a request will be complied with except where the College has a legal, contractual or public interest duty to retain the data or where such data may be required by outside agencies (e.g. HMRC)
- be informed if there is a breach of data security leading to data security being compromised

These principals are enshrined in the General Data Protection Regulation and the College treats security of data as a top priority. Provisions have been put in place to ensure that risks associated with holding data have been minimised.

The Regulation also includes information on rights of the data subjects. These are:

- Right to be informed,
- Right of Access,
- Right to Rectification,
- Right to Erasure,
- Right to Restrict Processing,
- Right to data portability,
- Right to Object and
- Rights in relation to automated decision making and profiling.

Data Register and Risk Analysis

A data register has been established which details all the type of data the college holds together with the security measures in place to ensure the data is protected.

The register gives a description of the data / service held, the categories of data included (name, address etc) and the reason why such data is retained. For example, collecting and retaining student information is a legal or contractual requirement whilst they are at college.

Where data is transferred to a third party this will be logged on the register, alongside the method of transfer and the format in which it is sent.

The collection and retention of data on individuals, be they students or staff, is a necessary part of the operation of the College. This may fulfil both a legal and contractual duty but also assists in the safeguarding of our students. The data register records how that data is secured. That may be through encryption of the data before it is processed, physical security (for example sensitive, paper based information may be stored in locked cabinets) or through restricted user access where that is appropriate and possible.

As part of the College's ongoing commitment to data security, the Data Register will be scrutinized by the Risk Management Team so that any associated risks can be discussed and procedures put in place to ensure the information is as secure as possible.

The current security measures and the implementation of any new procedures will help to mitigate the risk posed by retaining data. Whilst the risk of data loss cannot be completely eliminated, these procedures are designed to provide comfort to Data Subjects that information is being treated with the utmost care.

Privacy by Design

In the digital world, the College needs to continue to evolve to meet the challenges of data privacy. Stakeholders may request data to be divulged in different formats than currently available and the College has to be able to respond to those changes in a timely manner.

In any project that involves data collection or processing, applying the Privacy By Design principles ensures that the approach recognises the importance of promoting privacy and data protection compliance from the outset.

Privacy by Design might include projects such as building new IT storage systems, sharing information with a third party (such as a local authority) or merely manipulating current data into another form and storing that data in a different way.

Using the Privacy by Design approach helps the College to meet its obligations under the GDPR act but also demonstrates to Data Subjects that the security of their information has been assessed and any risks associated with holding that data has been minimised. It also means that data protection is addressed early and designs for systems can be altered to give comfort around data security.

Under this policy, staff must ensure that when they determine the need collect data they answer a number of questions early. For example, what data do I actually need (don't collect information that is not required), why are we collecting the data, how will it be stored, who will have access to that information, what safeguards are in place to reduce the risk of data breach?

Privacy Impact Assessment

The Privacy Impact Assessment is an integral part of the Privacy By Design approach. This helps identify risks of a process and aid decisions and design to eliminate, reduce or accept associated risk elements.

Below are a range of questions, taken from guidance issued by the Information Commissioner, which should be considered as part of any project to determine whether a Privacy Impact Assessment would be worthwhile.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records
- Will the project require you to contact individuals in ways which they may find intrusive?

If it is deemed necessary to carry out a Privacy Impact Assessment there are a number of basic steps to follow:

- What is the reason for collecting the information?
- What are the information flows associated with the project?
- What format will the information be in?
- Depending on the format, who within College should be consulted regarding its safekeeping?
- Can the information be anonymised and still be fit for purpose,
- Has the information collection been advised to the Data Protection Officer and therefore added to the Data Register.

Possible risks with a project might range from physical safety to distress caused to loss of material assets – ie financial loss as a result of data being compromised. Other risks might include:

- Inadequate disclosure controls could increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge. Just because data is secure in one area don't lose sight of how it might be downloaded and used elsewhere
- New surveillance methods may be an unjustified intrusion on their privacy. (ie CCTV cameras in new areas of College
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- If a retention period is not established information might be used for longer than necessary.

If, having carried out a Privacy Impact Assessment and despite mitigating processes being put in place, the risk to privacy is unacceptable, the viability of the project must be called into question.

Data Breaches

Under GDPR the College must report certain types of personal data beach to the relevant authority within 72 hours of learning of the breach. For certain types of breach, where a Data Subject's rights and freedoms might be compromised, all those affected must be informed.

The College has a procedure in place specifically related to data breaches and the recording thereof which includes:

- How to recognize a data breach,
- Recognising that a data breach does not just relate to a loss or theft of personal data,
- A response plan to ensure that, where breaches occur, the necessary steps are in place to address the breach and inform the relevant authorities and those affected by any such breach,
- A protocol relating to the organisational escalation in the event of a breach,
- Training of staff so they know the College has a dedicated person responsible for managing the response to a data breaches.

Subject Access Request & Data Portability

Staff, students, and other College users have the right to access any personal data that is being held about them, either on computer or paper-based files.

Staff can view their own computer based personal data via Columbus by clicking on the menu link 'My Personal Information'. Staff requiring access to view their own paper records should contact the Human Resources Manager.

Students can view their own computer based personal data through the Colleges Online Learning Platform. Students who wish to see their paper records should see their Pastoral Manager.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month in term time, or six weeks outside of term time, unless there is good reason for delay. In such cases the reason for delay will be explained in writing to the person making the request. The College will not make any charge for providing this information.

The individual is not entitled to access information about another person.

The College will provide all information it holds on a data subject in a readily recognizable format, such as a pdf.

Request for Information to be Removed

Under GDPR, staff and students have the right to request that information held about them is removed from College systems. The College will abide by any such requests if it is made in writing, and signed by the individual. The College will remove all data pertaining to an individual, except where it has a legal, contractual or public interest duty to retain information or where such information is required to enable the College to meet funding conditions.

Upon receipt of such a request, the College will advise the individual that such a course may have implications in the future should the individual request data that has been destroyed. The College will also advise which information it will retain where it is obliged to retain such information in order to comply with other legislation (e.g. HMRC).