Doncaster College | University Centre

North Lindsey College

DN COLLEGES GROUP

# Data Protection Policy

## 1. Purpose

1.1 The purpose of this policy is to ensure that DN Colleges Group (DNCG) is compliant with Data Protection Act 2018 (DPA 2018), United Kingdom General Data Protection Regulation (GDPR) and associated legislation. This policy incorporates guidance from the Information Commissioner's Office (ICO) and other relevant organisations.

The Policy provides a framework for compliance and will be supported by a series of additional policies and guidance documents focussing on specific areas of data compliance within DNCG.

The guidance documents will be used to provide advice and keep staff up to date with good practice.

## 2 Scope

2.1 This policy sets out how DNCG meets its obligations with regards to personal data (including Special Category data) as defined by Data Protection Act 2018 (DPA 2018), United Kingdom General Data Protection Regulation (GDPR) and associated legislation. Personal data is any information relating to a living individual who can be directly or indirectly identified, by reference to a personal identifier, such as a name, an identification number, location data, or an on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

This policy applies to all managers, staff, students, customers, governors, associates, partners, sub-contractors and any other colleagues and suppliers working for, or on behalf of DNCG.

It provides guidance on implementing the DNCG Data Protection Policy and the processing of personal data to comply with data protection legislation and with respect for confidentiality.

Data protection laws exist to strike a balance between the rights of individuals to privacy and the ability for organisations such as DNCG to use data for legitimate purposes.

## 3 Responsibilities

3.1 **Chief Executive Officer** – the CEO has overall accountability and responsibility for data protection. Operational responsibility is delegated to the Data Protection Officer and the CEO is responsible for ensuring that the role is performed.

**Data Protection Officer** – The DPO for DNCG has operational responsibility for the implementation of this policy and supporting procedures throughout the organisation and is the initial point of contact for any Data Protection related enquiries.

The DPO must also be adequately trained and sufficiently well-resourced in order to perform the role and is given the required independence to perform their tasks.

**Managers** – All Managers are responsible for ensuring that staff within their department are fully aware of, and abide by, this policy and any specific requirements relating to their roles and that staff have completed any Data Protection training that DNCG implements to support Data Protection.

**All Staff** – All staff have a responsibility for ensuring that any personal data which they hold is kept securely, transported safely (where this has been approved by the DPO) and that personal information is not disclosed in any way to any unauthorised parties. Personal data can either be electronic or paper based. All staff have a duty to report any data breaches or near misses relating personal data as soon as they become aware of them.

For the purpose of this policy "aware" is defined as when a member of staff has a reasonable degree of certainty that an incident has occurred which has resulted in personal data being compromised.

All staff are under legal and contractual obligations to keep personal and other information confidential not only during their employment (or equivalent) but also after it has been terminated.

**All Students, Staff and Other Parties –** Students, staff and other parties are responsible for ensuring that all personal data provided to DNCG is accurate and up to date.

## 4 Definitions and/or Relevant Legislation

| | | |
|---|---|---|
| 4.1 | Data Protection Legislation | Data Protection Act 2018 (DPA 2018)<br>United Kingdom General Data Protection Regulation (GDPR) |
| | Data Subject | Means people to whom data relates: all prospective, current and previous employees, learners, customers, sub-contractors, partners, suppliers, contacts, governors, referees, friends or family members of employees and learners. |
| | Data Controller | Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. |
| | Data Processor | Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. |
| | Processing | Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| | Personal Data | Any information in relation to an identified or identifiable living individual. "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual. |
| | Special Categories of Personal Data | Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. |
| | Criminal Convictions and Offences Data | Personal data relating to criminal convictions and offences under Article 10 (GDPR). |

| | |
|---|---|
| Employees | All current, previous and prospective members of staff. |
| Students | All current, previous and prospective customers, clients, participants or programme participants. In some parts of DNCG the term “Learners” is also used and will be taken to mean the same as “Students”. |
| Official Information | Information that relates to the organisation and its activities. |
| Supervisory Authority | The independent public authority responsible for data protection. The supervisory authority for DNCG is the Information Commissioner’s Office (ICO). |
| Privacy and Electronic Communications Regulations (PECR) | The Privacy and Electronic Communications (EC Directive) Regulations 2003. |

4.2 Relevant legislation:

- Data Protection Act 2018 (DPA 2018)
- United Kingdom General Data Protection Regulation (GDPR)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003

## 5 The Policy

### 5.1 Information Commissioner’s Office (ICO)

The ICO is the UK’s data protection regulator (Supervisory Authority).

As a data controller, DNCG is required to register with the ICO and submit an annual notification listing the purposes under which it processes personal information. DNCG must also notify the ICO within 28 days should any entry become inaccurate or incomplete. The ICO publishes a register of controllers on its website which is available to the public for inspection. Responsibility for maintaining these notifications rests with the Data Protection Officer.

DNCG’s registrations are as follows:

- DN Colleges Group - Registration No: ZA341759
- Optime Support Limited– Registration No: ZA885394

**Implementation**

To meet its responsibilities DNCG will:

- Ensure any new or planned projects that involve Personal Data are preceded with a Data Privacy Impact Assessment
- Ensure that access controls are limited to role relevance
- Ensure any personal data is collected in a fair and lawful way
- Gain explicit consent where required
- Explain at the outset why information is being collected, what it will be used for and with whom it will be shared
- Ensure that only the minimum amount of information needed is collected and used
- Ensure the information used is up to date and accurate

- Review the length of time information is held, in line with JISC recommendations and other relevant legislation
- Ensure information is kept safely
- Ensure the rights people have in relation to their personal data can be exercised
- Dispose of data appropriately and without unnecessary delay
- Ensure that anyone managing and handling personal information is trained to do so
- Ensure that anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do
- Any disclosure of personal data will be in line with relevant legislation, and internal policies and procedures
- Any regular formal sharing of data to third parties is covered by a data sharing agreement
- Take measures to ensure safe transfers of data outside of the UK where cross border sharing is necessary

**DNCG Personnel's General Obligations**

All Personnel must comply with this policy.

DNCG Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

DNCG Personnel must not release or disclose any Personal Data:

- outside the organisation; or
- inside the organisation to DNCG Personnel not authorised to access the Personal Data; or
- as required formally by their job role,

without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

DNCG Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other DNCG Personnel who are not authorised to see such Personal Data or by people outside the organisation.

**Data Protection Principles**
When using Personal Data, Data Protection Laws require that DNCG complies with the following principles. These principles require Personal Data to be:

| **Data Protection Principles** | **How DNCG Complies** |
|---|---|
| Lawfulness, fairness and transparency | DNCG issues Privacy Statements explaining how it processes data at the point of capture and for what purposes. |
| Purpose limitation | DNCG shall only use personal data for the purposes for which it was collected. |
| Data minimisation | DNCG shall only collect personal data relevant to the purpose for which it is required. |
| Accuracy | DNCG shall ensure the data it processes is correct, up to date and able to be rectified promptly. |
| Storage limitation | DNCG shall not store data for longer than it is required. |

| | |
|---|---|
| Integrity & confidentiality | DNCG implements various measures to protect personal data from unauthorised access, loss or destruction. |

All DNCG employees are responsible for ensuring that the above Data Protection Principles are observed at all times and at all stages of the data lifecycle including:

- Collection or capture of personal data
- Post collection processing of data e.g. storing, alteration, transmission etc.
- Erasure or destruction of personal data

DNCG is required by law to be able to demonstrate compliance with the Data Protection Principles and has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that DNCG can demonstrate its compliance.

**Records of Processing Activities**

"Processing" is the collection, recording, organisation structuring, storage, adoption or alteration, retrieval, consultation or use, disclosure, destruction or erasure of personal data.

DNCG will identify the legal basis for processing 'personal data' as defined by Article 6 and 'special categories of data' as defined by Article 9 and document this on a Record of Processing Activity (ROPA) through an Information Asset Register as required by Article 30.

DNCG will assess which lawful purpose applies to make each use of personal data lawful. If the use changes then the assessment will need to be redone. The use of personal data will be reviewed periodically, and any initial data audits will be updated periodically too. If we are considering making changes, we will decide whether their intended use requires amendments to be made and any other controls which need to apply, and we may need to notify Individuals (Data Subjects) about the change.

**Lawful Basis for Processing Personal Data**

In order to process Personal Data lawfully, DNCG must meet one of the lawful bases for processing. The lawful basis must be established before processing begins.

The six lawful bases are:

- **Consent:** DNCG should be able to demonstrate that the data subject has provided recent, clear, explicit and defined consent for their data to be processed for a specific purpose.
- **Contract:** The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- **Legal Obligation:** The processing is necessary for compliance with a legal obligation to which DNCG is subject.
- **Vital Interest:** The processing is necessary in order to protect the vital interests of the data subject or of another natural person. E.g. to protect an individual's life.
- **Public Interest:** The processing is necessary for DNCG to perform a task in the public interest or for official functions and the task or function has a clear basis in law.
- **Legitimate Interest**: The processing is necessary for the purpose of the legitimate interests of DNCG or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data.

**Lawful Basis for Processing Personal Data - 'Special Categories of Personal Data'**

In addition, when DNCG collects and/or uses Special Categories of Personal Data, we must demonstrate that one of a number of additional conditions is met. These are set out in Article 9 and are as follows:

- Explicit consent
- Employment and social security obligations
- Vital interests
- Necessary for establishment or defence of legal claims
- Substantial public interest
- Various scientific and medical issues.

If DNCG changes how it uses Personal Data, it needs to update this record and may also need to notify Individuals about the change. If DNCG Personnel therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

**Deciding on the Appropriate Condition for Processing**

When a member of DNCG Staff are assessing the lawful basis for processing data, they must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. DNCG cannot rely on a lawful basis if they are able to reasonably achieve the same purpose by some other means.

Remember that more than one basis may apply, and DNCG should rely on what will best fit the purpose, this may not always be the easiest.

**Individuals' Rights**

The UK GDPR gives individuals more control about how their data is collected and stored and what is done with it, in the form of "individual rights", DNCG must ensure all procedures that involve the processing of personal data can demonstrate how individuals can exercise these rights.

Individuals can request to exercise these rights verbally or in writing. When a request to exercise any of the following rights is received by a member of staff, they must inform the Data Protection Officer immediately.

**The Right to be Informed**

- Individuals have the right to be informed about the collection and use of their personal data.
- DNCG provides Privacy Notices to meet this requirement.

**The Right of Access**

- Individuals have the right to request access to their personal data.
- The is often called a Subject Access Request.

**The Right to Rectification**

- Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete.

**The Right to Erasure**

- Also known as the right to be forgotten, this enables individuals to request their data be erased.

- This is not an absolute right and only applies in certain circumstances.

**The Right to Restrict Processing**

- Individuals have the right to request the restriction or suppression of processing of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, DNCG are permitted to store the personal data, but not use it.

**The Right to Data Portability**

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- The right only applies to information an individual has provided to a Controller (DNCG).
- It allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.

**The Right to Object**

- This gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In some cases, where the right to object applies DNCG may be able to continue processing if there is a compelling reason for doing so.

**Rights in relation to Automated Decision Making and Profiling**

- Automated decision making is using solely automated methods without any human involvement in order to make a decision about an individual.
- Profiling is any form of automated processing that uses personal data to analyse or evaluate certain personal aspects relating to an individual.

DNCG can only carry out this kind of processing if the decision is:

- Necessary for the entry into or performance of a contract.
- Authorised by domestic law applicable to the data controller.
- Based on the individual's explicit consent.

In order to process data in this manner, DNCG shall ensure that:

- Individuals receive information about the processing.
- There are simple ways for the individual to request human intervention or challenge a decision.
- Regular checks are carried out to make sure that the systems are working as intended.

DNCG Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

DNCG does not carry out Automated Decision Making or Profiling in relation to its employees.

The most commonly exercised individual right is that of the right of access. The right of access allows an individual to know what information DNCG holds and processes about them. This is known as a subject access request, which also allows individuals to be given a copy of the information held, as well as supplementary information, such as where and with whom the information may have been shared. The right of access, like many of the individual rights, is not an absolute right and disclosure of the requested information is subject to exemptions.

Unless the information requested is provided as part of the normal course of business, the individual who is the subject of the data (the data subject) should be directed to the DPO who can be contacted at dataprotection@dncolleges.ac.uk for advice on how to make a Subject Access Request (SAR). DNCG must respond to these requests within one month of their receipt.

**Transparent Processing – Privacy Notices**

Personal data must be processed 'in a transparent manner'. This is achieved by providing the data subject with information at the point of data capture, or if this is not possible, within a reasonable period after obtaining the data, but at least within one month. This information is known as a Privacy Notice.

If DNCG receives Personal Data about an Individual from other sources, it will provide the Individual with a privacy notice about how DNCG will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

If DNCG changes how it uses Personal Data, DNCG may need to notify Individuals about the change. If DNCG Personnel therefore intend to change how they use Personal Data please notify the Data Protection Officer who will decide whether the intended use can be permitted and requires amendments to be made to the privacy notices and any other controls which need to apply.

**Marketing and Consent**

DNCG will sometimes contact Individuals to send them marketing or to promote the College. Where DNCG carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

Marketing consists of any advertising or marketing communication that is directed to particular individuals. Data Protection Act 2018 brings about a number of important changes for organisations that market to individuals, including:

- providing more detail in their privacy notices, including for example whether profiling takes place; and
- rules on obtaining consent require an individual's "clear affirmative action". The ICO expects consent to be used in a marketing context.

DNCG also need to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection. PECR apply to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data (cookies)

DNCG will either use an un-ticked opt-in box for consent, or alternatively, may use a "soft opt in" if the following conditions are met:

- contact details have been obtained in the course of a sale (or negotiations for a sale);
- is marketing its own similar services; and
- has given the individual a simple opportunity to opt out of the marketing, both when first collecting the details and in every message after that.

**Training**

DNCG will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

The Data Protection Act 2018 will be a mandatory training module for all staff and successful completion will be a requirement of their employment.

Individuals whose roles require regular access to special category data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

**Data Security**

DNCG takes information security very seriously and has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. DNCG has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

**Data Breach**

Whilst DNCG takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and DNCG Personnel must comply with DNCG's Data Breach Notification Process.

Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal to the organisation does.

There are three main types of Personal Data breach which are as follows:

**Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that DNCG Personnel are not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person, to third parties who are ineligible to receive the information or who are eligible in general but not to specific information given;

**Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransomware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

**Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

**Data Protection Impact Assessments (DPIA)**

The Data Protection Act 2018 introduces a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (**"DPIA"**). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition

on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and
- the measures to address the risks.

Where a DPIA reveals risks, which are not appropriately mitigated the ICO must be consulted.

Where DNCG is launching or proposing to adopt a new process, product or service which involves Personal Data, DNCG needs to consider whether it needs to carry out a DPIA as part of the project initiation process. DNCG needs to carry out a DPIA at an early stage in the process so that DNCG can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

Situations where DNCG may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

- large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling where legal or similarly significant decisions are made;
- large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or
- systematic monitoring of public areas on a large scale e.g. CCTV cameras
- Introduction of an IT system which processes large amounts of personal data

All DPIAs must be reviewed and approved by the Data Protection Officer.

**Data Retention**

The UK GDPR does not dictate how long DNCG should keep personal data however, one of the data protection principle states that "*data should be kept in a form which permits identification of a data subject for no longer than is necessary*." This means that the data must only be stored for as long as it is required. DNCG shall determine the suitable retention period for data being processed and ensure that once this data has reached this threshold, it is securely destroyed, anonymised or erased. The retention period of the data will be determined by the purpose for which it is processed and the lawful basis for processing it.

For data processed by DNCG, the retention period and any relevant justifications are recorded in the DNCG Document Retention Schedule. It is the responsibility of Managers to ensure that both paper and electronic records are retained or disposed of accordingly. Disposal of any paper documents must be done by using confidential waste disposal sacks provided by Estates.

**Appointing Contractors Who Access the College's Personal Data**

If DNCG appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that DNCG only appoints them where they have carried out sufficient due diligence and only where appropriate contracts are in place.

One requirement of Data Protection Act 2018 is that a Controller must only use Processors who meet the requirements of the Data Protection Act 2018 and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed, they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

Any contract where an organisation appoints a Processor must be in writing.

DNCG will be considered as having appointed a Processor where they engage someone to perform a service as part of it they may get access to Personal Data for which you are the responsible controller. Where DNCG appoints a Processor DNCG, as Controller remain responsible for what happens to the Personal Data.

Data Protection Act 2018 requires the contract with a Processor to contain the following obligations as a minimum:

- to only act on the written instructions of the Controller;
- to not export Personal Data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- to keep the Personal Data secure and assist the Controller to do so;
- to assist with the notification of Data Breaches and Data Protection Impact Assessments;
- to assist with subject access/individuals rights;
- to delete/return all Personal Data as requested at the end of the contract;
- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of the Data Protection Act 2018 or other EU or member state data protection law.

In addition, the contract should set out:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of Personal Data and categories of individuals; and
- the obligations and rights of the Controller.

## 6 Relevant Policies and Procedures

6.1 **Privacy Statements:**

The following Privacy Statements are in use across DNCG:

- Student
- Staff
- Governor
- Fitness Suite Member
- Kingsway Nursery
- Covid-19

**Appendices:**

Appendix 1 - Staff Guidelines for Data Protection
Appendix 2 - Staff Checklist for Recording Data
Appendix 3 – Access to Information (Subject Access Request) Form

## 7 Who to Contact with Queries

7.1 Any questions or concerns about the interpretation of this policy and how it relates to a staff members area of work should be referred to their line manager or the Data Protection Officer.

Data Protection Officer – dataprotection@dncolleges.ac.uk

## 8 Communication

8.1 The policy will be communicated to all staff via the College(s) Intranet, staff training and Email.

## 9 Authorisation

| | |
|---|---|
| Policy Holder: | Data Protection Officer |
| Approval Committee: | Senior Leadership Team |
| Approval Date: | 23 June 2021 |
| Next Review Date: | 23 June 2024 |

**Appendix 1 - Staff Guidelines for Data Protection**

Staff process data about students on a regular basis when marking registers, writing reports or references, or as part of a pastoral or academic supervisory role. The College will ensure through admission and registration procedures that all students give their consent to this sort of processing as necessary and are notified of the categories of processing as required by the Act. The information that staff deal with on a day-to-day basis will be “standard” and will cover categories such as:

- general personal details such as name and address
- details about class attendance, course work marks and grades and associated comments
- notes of personal supervision including matters about behaviour and discipline

Information about a student’s physical or mental health; sexual life; political or religious views; trade union membership, ethnicity or race is sensitive (‘special category’ data) and can in most cases only be collected and processed with the student’s explicit consent. For example, recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties. Wherever possible, this information should not be held by individual staff but instead recorded appropriately within the college’s official database systems.

All staff have a duty to make sure that they comply with the data protection principles which are set out in the College’s Data Protection Policy. In particular staff must ensure that records are:

- accurate
- up-to-date
- fair
- kept and disposed of safely, and in accordance with the College’s policy (using ‘confidential waste’ facilities)

Staff must not disclose personal data to any student, or third party, without authorisation from the data subject, agreement from the designated data protection officer or in line with College policy.

Staff shall not disclose personal data to any other staff members except with the authorisation of the data subject, agreement of the designated data protection officer or in line with College policy.

Before processing any personal data, all staff should consider the checklist and tips at Appendix 2.

**Appendix 2 - Staff Checklist for Recording Data**

- Do you really need to record the information - use ProSolution Web / ProMonitor instead?
- Is the information ‘standard’ or sensitive?
- If it is sensitive (special category) data, do you have the data subject’s explicit consent?
- Has the individual been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- Do you have authorisation from the relevant college authorities to hold and maintain electronic records outside of the college’s official systems?
- If you do not have the data subject’s consent to process, are you satisfied that it is in the best interests of the student or staff member to collect and retain the data?
- Have you reported the fact of data collection to the authorised person within the required time?

Tips for protecting and using information

- Keep passwords secure and not easy to guess – change regularly, never share with other staff or students
- Lock or log-off computers when away from desks/working areas
- Use data on computer screens appropriately – think who can see the computer monitor?
- Prevent virus attacks by being careful when opening emails/attachments and visiting websites
- Securely store hard copy information – not just left lying around on desks
- Accompany visitors and students if they need to visit staff-restricted area

**Appendix 3 – Access to Information (Subject Access Request) Form**

I, (insert name) _____ wish to have access to either:
*(please tick as appropriate)*

☐ All the data that the College currently has about me, either as part of a computerised system or part of a relevant paper-based filing system

Or data that the College has about me in the following categories (*please tick):*

☐ Academic marks or course work details

☐ Academic or employment references

☐ Disciplinary records

☐ Health and medical matters

☐ Political, religious or trade union information

☐ Any statements of opinion about my abilities or performance

☐ Personal details including name, address, date of birth etc.

☐ Other information (please specify)

I am *(please tick)*: ☐ Student ☐ Member of staff
☐ Other (please specify)

*While the College will endeavour to comply with data subject access requests as quickly as possible, it is able to respond more effectively to specific requests than general requests. In all cases, the request will be processed within the 30 day limit specified under the Act.*

| |
|---|
| Name *(please print)* |
| Contact telephone number/email |
| Address |
| Signed Date |
| **After identification has been verified, this form must be forwarded to the designated data protection officer.** |