POLICY

Title: Data Protection

Policy Holder: Director of Governance and Legal

Approval Board: College Leadership Team

Version No: v3.0

Last reviewed: January 2024

Review period[1]: 2 Years

Summary: This policy aims to explain the requirements of the legislation, sets out the expectation for compliance, and signpost relevant procedures and guidance notes to support staff.

Accessibility: If you would like this information in an alternative format, e.g. Easy to Read, large print, Braille or audio tape, or if you would like the procedure explained to you in your language, please contact the College's marketing team on 01603 773 169.

Further information: If you have any queries about this policy or procedure, please contact the named policy holder or the College's marketing team on 01603 773 169.

EASTON COLLEGE PASTON COLLEGE CITY COLLEGE NORWICH

City College Norwich, Ipswich Rd, Norwich NR2 2LJ

Legislation or Regulation:	• UK General Data Protection Regulation • Data Protection Act 2018 • Privacy and Communications (EC Directive) Regulations 2003 • Computer Misuse Act 1990 • Freedom of Information Act 2000 • Protection of Freedoms Act 2012 • Investigatory Powers Act (2016) • Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000

Version Control Document			
Date	**Version No.**	**Reason for Change**	**Author**
Jan 2017	v 2.0	Rewrite / Incorporate 'current legislation'	D.Clarke
May 2017	v 2.3	Review	P.Beacock
Nov 2017	v 2.4	Contact number updated	P.Beacock
May 2018	v 2.5	Updated to reflect changes in legislation/regulation	P.Beacock
Aug 2019	v 2.6	Removal of UTCN References	P.Beacock
Jan 2021	v 2.7	Review	J.Mitchell
Mar 2021	v 2.8	Removal of TEN Group references	P.Beacock
Dec 2021	v 2.9	Removal of NES references	P.Beacock
Nov 2022 / Jan 2024	v 3.0	Review	Info Compliance

[1] The Review Period refers to our internal policy review process. The published policy is current and is the most recent approved version.

Contents

1. Policy Statement 4

2. Policy Aims & Objectives 4

3. Definitions 4

4. Scope 5

5. Legal Requirements 6

6. Procedure 6

7. Organisational Responsibilities 16

8. Reference to other relevant policies and procedures 17

9. Contact 17

10. Equal Opportunities Statement 17

Appendix 1 Relevant Legislation 18

Appendix 2 Data Protection Impact Assessment (DPIA) 20

Annex A – Examples of individual, organisational and compliance risks 27

Annex B - Evaluation of risk 28

Annex C – Example measures to reduce risk 29

Annex D – Special Category or 'High Risk data' 30

Annex E - DPIA Risk Matrix 31

Annex F – Examples of Low, Medium and High Risk Personal Data 33

1. Policy Statement

City College Norwich ("The College") is committed to fostering high standards of data protection in all processing of personal data relating to employees, students, contractors and visitors. In particular, the College will work to ensure that all legal obligations under the General Data Protection Regulation (GDPR) and successor legislation are met by all organisations.

The CCN Board actively promotes a culture whereby the principles of the UK GDPR and the Data Protection Act 2018 (DPA2018) are known, understood and embedded into day to day processing, and that data protection/privacy considerations are acknowledged early in the planning of any new or changed activity so that exposure to risk is minimised and/or managed.

2. Policy Aims & Objectives

This policy aims to explain the requirements of the legislation, sets out the expectation for compliance, and signpost relevant procedures and guidance notes to support staff.

The policy sets out the following objectives for all the College:

- ensure that personal data is processed fairly and lawfully, and only for specified purposes, using an information asset register to record processing activities;
- allocate specific responsibilities for data protection compliance;
- ensure that privacy impact assessments are undertaken for new or changed processing involving personal data;
- implement a data protection compliance system to include regular audits, inspections and a review of actions arising;
- ensure that appropriate Data Sharing Agreements are in place where regular sharing of personal data takes place;
- undertake effective preliminary checks and implement Data Processor Agreements where third-party processors are engaged;
- ensure adequate notification and communication to staff, students or parents on the processing of their personal data;
- ensure appropriate procedures are in place to respond to individuals who are exercising their rights under relevant legislation;
- provide adequate information instruction and training for staff who are processing/handling personal data;
- ensure any incidents or breaches involving personal data are recorded, investigated and, where appropriate, reported to the regulator;
- provides adequate resources to deliver secure processing of personal data undertaken at any of their managed sites or at any other workplace.

3. Definitions

3.1 Personal Data

The UK GDPR defines personal data as information that:

- Identifies[1] a living individual;
- is stored and used electronically, or within structured manual records, and includes accessible records such as education or health records;
- includes an expression of opinion about or intention towards a person.
- Personal Data that has been pseudonymised – e.g. Key-Coded – can fall within this scope depending on how difficult it is to attribute the pseudonym to a particular individual is.

[1] The individual can be identified from the information itself, i.e. it includes their name, or when linked with other information that we hold, e.g. under a unique reference number.

3.2 Sensitive Personal Data (Special Category)

The UK GDPR refers to sensitive personal data as "special categories data" and specifies this data as:

- Racial or ethnic origin
- Biometric data
- Genetic data
- Political opinion
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sex life
- Sexual orientation
- Commission of offences or alleged offences

This type of data is subject to further regulation under the UK GDPR and can be processed only under certain circumstances.

3.3 Processing

Processing is any activity involving personal data. This includes obtaining, recording, transferring, storing, retrieving, consulting, amending, printing, deleting, and destroying.

3.4 Data Subject

The individual to whom the information relates.

3.5 Data Protection Officer (DPO)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the compliance of the College with data protection law, and developing related policies and guidelines where applicable.
The DPO is also the first point of contact for individuals whose data the College process, and for the ICO.

3.6 Data Controller

The person/organisation who, either alone or jointly or in common with others, determines the purposes and manner of the processing of personal data. This is usually the organisation, company etc which is the controlling legal entity. Functions can be delegated to senior designated individuals. The governing body/board is a Data Controller for their organisation.

3.7 Data Processor

Any person (other than an employee of the Data Controller) who processes personal data on behalf of the Data Controller.

3.8 Third Party

Any person/organisation external to the Colleges trustees, employees, and the data subjects.

4. Scope

This policy relates to all personal data created, received or maintained or in any way processed by staff working for the College in the course of their duties. It further applies to all personal data created, received or maintained by external parties/contractors on behalf of the College.

5. Legal Requirements

UK General Data Protection Regulation (UK GDPR) / Data Protection Act 2018 (DPA 2018)
The UK GDPR and the DPA 2018 are the primary legislation covering personal information. They require that the processing of personal data complies with all of the principles specified under Article 5 of the UK GDPR, as follows:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

The GDPR is retained in domestic law post Brexit but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018.

Other legislation creates additional requirements relating to types and/or processing activities of personal data:

- Privacy and Communications (EC Directive) Regulations 2003 which apply to the use of personal data in direct marketing and other use of electronic communications,
- Computer Misuse Act 1990 which relates to unauthorised access or modification to computers,
- Freedom of Information Act 2000, which provides for access to all information held by public authorities;
- Protection of Freedoms Act 2012 which imposes specific requirements in relation to the biometric information.
- Regulation of Investigatory Powers Act (2000)
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Legislation relating specifically to education also has implications for the processing of personal data. Further information is available at Appendix 1.

6. Procedure

6.1 Monitoring the Implementation and Effectiveness of the Policy

The Director of Governance and Legal and the Information Compliance team monitors the effectiveness of this procedure through audit, acting on reports received, preparation of data incident statistics and statistics relating to Data Protection Impact Assessments and information requests as required. The Director of Governance and Legal reports to the applicable Data Controllers and reports recommendations for action if necessary.

6.2 Registration with the ICO and the Data Protection Fee

The College is registered with the Information Commissioner's Office for the processing of personal data, with renewals managed by the Information Compliance team. The College will inform the Information Compliance team of any changes to processing activities so the registration can be updated as necessary.

Organisations are now required register and potentially pay the ICO a data protection fee unless they are exempt. The new data protection fee replaces the requirement to 'notify', which was covered by the

Data Protection Act 1998. The ICO have the power to enforce the 2018 Regulations and to serve monetary penalties on those who refuse to pay their data protection fee.

6.3 Privacy by Design / Privacy by default

The College has measures in place to show that they have integrated data protection into all of their data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in the UK GDPR
- Completing Data Protection Impact Assessments (DPIAs) where the organisations process of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Developing IT systems, services, products and processes that involve processing personal data
- Developing organisational policies, processes, business practices and/or strategies that have privacy implications
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the contact details of the College DPO and all information the College are required to share about how they use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

6.4 Data Protection Impact Assessments

Data Protection Impact Assessments (DPIAs) are a form of risk assessment and a process for undertaking a DPIA based on the standard risk assessment is shown at Appendix 2. As a requirement of the UK GDPR, DPIAs will be integrated into the planning of all new projects or activities which involve the processing of personal data and are likely to result in a high risk to individuals, this may include the use of new technology related to personal data processing or new arrangements for processing personal data e.g. working off-site. Implications for privacy and data protection are considered at an early stage and the measures to address risks are recorded together with control measures. The Project Leader/Manager responsible for the project or the area of activity undertakes the privacy risk assessment in consultation with stakeholders and the Information Compliance team.

6.5 Staff Training and Awareness

College Induction sessions for all new staff includes information about data protection and the handling of personal information.

All staff are required to complete mandatory Data Protection Core Training, via an online module or a one hour session delivered by the Information Compliance team, with the training repeated every two years. The Principal and Managers are responsible for ensuring that staff complete the training and have sufficient time allowed. The College Training and Development team monitor completion figures and report to Principal/Managers on a regular basis. Staff who fail the end of course test twice or more are referred to the Information Compliance team for additional training. Persistent failure to pass the training may be dealt with as a performance issue, persistent failure to undertake the training will be dealt with as a disciplinary matter.

Additional and bespoke training sessions can be provided by the Information Compliance team on request, and as identified via DPIAs, audits and staff development needs analysis.
Information about data protection compliance measures as well as support material is made available to staff using the intranet.. Requests for information in alternative formats should be made to the Information Compliance Team.

6.6 Audit

The Information Compliance Team undertake audits of the College's compliance with the legislative requirements and this policy. Following an audit, an action plan for improvement is developed and agreed with the organisation.

6.7 Privacy Notices and Communication to Data Subjects

Privacy notices and communication with data subjects about how their personal data is being processed is a requirement under Articles 12, 13, 14, 15 to 22 and Article 34 of the UK GDPR. The Information Compliance team produce a privacy notices for the College, which is published on College websites and can be issued with Admissions Forms or at other appropriate points when information is being collected. A privacy notice contains the following information:

- details of the Data Controller;
- all purposes for processing of personal data;
- with whom personal information will be shared.
- The rights of the data subject in relation to their personal data

New arrangements to collect and/or use personal data will require additional notification to data subjects and amendment to the published privacy notice. Managers are to ensure that hard copy/electronic forms and other technologies which are used to gather personal data are accompanied by privacy notices at the point of collection.

Privacy notices relating to the processing of staff personal data are published on the intranet under the Communications tab.

Privacy notices should be in a format and style appropriate for the audience, particularly to ensure they are easily understood by the various age groups of our students.

6.8 Lawful Processing, Consent and Right to Erasure ('right to be forgotten')

Lawful Processing

The primary function of the College is that of education, either as a provider or in support of the providers. In order for the use of personal data to be lawful, the purpose should relate to:

1. a legitimate and justified function of an educational establishment, and
2. the articles of corporation or funding agreement for the establishment, and
3. meet a condition for processing established by Article 6 (and Articles 9 and 10 where necessary) of the UK GDPR.

Consent

Where the purpose for using personal data does not fall within points 1 and 2 above and there is no legal obligation for the processing, it may be necessary to obtain consent from the individual(s). Consent should be obtained only when it can be given freely and be equally freely withdrawn without causing detriment to the individual. Consent should not be used purely as a 'safety net' to legitimise the processing, but only when there is no other justification for the processing.

Under the UK GDPR the use of consent attracts additional rights, including the right for all data to be deleted when consent is withdrawn in certain circumstances, and therefore it will be important to ensure it is used only when appropriate.

Where online services are made available to students, such as classroom apps, and the intention is to rely on consent as a basis for processing, parental consent may be sought in certain circumstances (except for online counselling and preventive services).

Right to Erasure ('right to be forgotten')

Under Article 17 of the UK GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the UK GDPR.

6.9 Limitation, minimisation and accuracy

The College will only collect personal data for specified, explicit and legitimate reasons. These reasons are explained when data is initially collected.

If the College wish to use personal data for reasons other than those given when first obtained, they will inform the individuals concerned before they do so and seek consent where necessary.

College staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the organisations records management retention schedule.

6.10 Use of Personal Images, Photographs and Videos

Photographs and images of people can capture the distinguishing features of an individual which identify them. The College will also have information such as name etc. which they can link to the image to enable further identification. Images can also be capable of being sensitive personal data, for example, if they can depict a person's racial or ethnic origin or show that a person has a disability.

The taking, using and sharing of personal images will be handled in accordance with Article 5 of the UK GDPR in the same way as other types of personal data. Students, staff and others must be informed of when and why personal images might be taken and/or used, and ask for consent when use of the

image is for a purpose not specific to the individual's education and is not covered by the organisation's privacy notice.

The College does not advocate a policy of a blanket ban of the taking of images by parents/carers etc. as a family record of their child's participation in college life. It will be for the college to decide on their approach, and this can be adjusted depending on the event and the students involved. It is expected that restricting parents/carers from taking images will be on an exceptional basis and in relation to specific, identified safeguarding needs. If restrictions are to be in place these are to be notified to visitors as soon as possible.

Further information is available in the Use of Personal Images Guidance Note published under the Communications tab.

6.11 Closed Circuit Television (CCTV)

Closed Circuit Television (CCTV) is widely used in the UK to enhance safety and security. The presence of CCTV can act as a deterrent to those intent on committing crime or other inappropriate behaviours against others or property, and communities can feel safer as a result. Images recorded by CCTV can be significant in the investigation and resolution of incidents, sometimes providing an unequivocal portrayal of events. However, it is accepted that CCTV is intrusive, providing an ongoing record of individuals' movements and activities. The usefulness of CCTV images can be much reduced by poor siting of equipment, and poor quality. For this reason, the College has put in place requirements to ensure the use of CCTV is fully and properly assessed, implemented and monitored in accordance with relevant legislation and codes of practice.

The College use CCTV only for the following purposes:

- To detect, prevent or reduce the incidence of crime
- To prevent and respond effectively to all forms of harassment (including bullying) and disorder
- To improve communications and the operational response of security patrols in and around the areas where CCTV operates
- To reduce the fear of crime
- To create a safer community
- To gather evidence by a fair and accountable method
- To provide emergency services assistance
- To provide assistance for internal investigations/disciplinary hearings within the institution for the purpose of safety and security of all campus users and their property.

With regard to internal investigations/disciplinary hearings, CCTV images will be used only when the alleged conduct is classed as 'gross misconduct' according to the organisation's employee and student conduct policies and the alleged conduct is deemed to have compromised the safety and security of individuals or property. For incidents not relating to gross misconduct, CCTV images can be used only with the consent of all relevant parties.

CCTV systems will not be used to monitor the performance of employees without their knowledge.

If the College wishes to change the use it makes of CCTV, it must contact the Information Compliance Team so that arrangements are made to amend the notification.

The College when using CCTV will ensure the following is in place:

- A Data Protection Impact Assessment has been conducted for any new/changed use
- Published Privacy Notice states that CCTV is in use and specifies the purpose(s) of its use
- A staff member is nominated as CCTV Manager and has responsibility for the operation of the CCTV system
- The Information Compliance Team is consulted and a CCTV Code of Practice is put in place

Further information is available in the CCTV Guidance Note and CCTV Code of Practice published under the Communications tab.

6.12 Personal Data and Social Media

Sharing an individual's personal data via social media (e.g. Twitter, Facebook etc) places information in the public domain which can be re-shared/retweeted multiple times and reach a huge audience. Care must be taken when using personal information in this way and, as well as ensuring any such use of personal data complies with the UK GDPR, staff should refer to the Social Media Policy for guidance.

6.13 Data Sharing Agreements

Where the regular exchange of personal data takes place with another organisation and where each organisation makes decisions relating to the personal data, a Data Sharing Agreement is negotiated. A Data Sharing Agreement is concerned purely with personal data and identifies:

- the legal basis and purpose for the data sharing
- a description of the data to be shared
- the responsibilities of each party in ensuring compliance with the UK GDPR
- security measures
- termination arrangements

Managers are to consult the Information Compliance team where the regular exchange of personal data occurs or is planned. Further information is available in the Personal Data Disclosure Guidance Note available under the Communications tab.

6.14 Data Processor Reviews and Agreements

Where a third party processes personal data on behalf of the College, a review of the third party data protection compliance arrangements is undertaken by the Information Compliance team, and, where appropriate, a Data Processor Agreement is negotiated. A Data Processor Agreement is concerned purely with personal data and ensures that:

- processing of personal data is only undertaken in accordance with instructions from the organisation and in accordance with the UK GDPR
- appropriate security measures are in place to safeguard the personal data from any unauthorised and unlawful processing, accidental loss, damage, alteration or disclosure
- the Data Processor has undertaken reasonable steps to ensure the reliability of personnel with access the personal data
- arrangements in relation to Subject Access Requests (SAR), complaints and breaches of the Data Protection Legislation.
- termination arrangements, including the disposal of the personal data

Data Protection Impact Assessments identify the need for a Data Processor Agreement at an early point in planning new activities which involves personal data.

Directors and Managers are to consult the Information Compliance Team in advance where a third party is to process personal data on the organisation's behalf or as part of a service which it plans to offer. Further information is available in the Disclosure of Personal Information Guidance Note available under the Communications tab.

6.15 Third Party Requests for Disclosure of Personal Data

Where ad hoc requests from third parties for the disclosure of information about an individual are received, these are not processed unless the request is in writing and one of the following applies:

- the condition(s) for processing have been met, e.g. a legal obligation, a contract, consent etc
- an exemption applies

In many cases, the consent of the Data Subject should be obtained. However, if the disclosure is required under a legal obligation, or an exemption is relevant, consent is not appropriate. Consideration should be given whether to notify the Data Subject(s) of the proposed disclosure, unless this would prejudice the purpose for the disclosure.

In some circumstances, a fee may be charged for the provision of information. A 'reasonable fee' can be levied for the administrative costs of complying with the request. A policy covering the Charging of Fees for the Provision of Information (Statutory Requests) is available under the Communications tab.

Disclosure of personal data to third parties is a complex area and all such requests are to be notified to the Information Compliance team who undertake the response to the request on behalf of the receiving organisation or will provide advice. Further information is available in the Disclosure of Personal Information Guidance Note available under the Communications tab.

Where there is a regular and routine need to share information between organisations, a Data Sharing Agreement is needed. (See item 6.13)

6.16 Subject Access Requests

All individuals (Staff, Students and other Data Subjects) have the right of access to personal data which an organisation holds about them. Individuals (or their nominees) can make the request verbally or in writing but must clearly state what personal data is being requested.

The Information Compliance team receives and processes subject access requests for the College. Requests are processed promptly and within one calendar month.

6.17 Professional Content

The legal definition of personal data includes 'expressions of opinion about the data subject, and intentions towards them' and information recorded in any format, including notes and emails. All information recorded about individuals will be professional in tone and content and will be accurate as far as is possible depending on the source of the information.

6.18 Complaints, Incidents and Breaches Involving the Processing of Personal Data

A breach of the UK GDPR (or other related legislation) occurs when personal information is not processed according to Article 5 of the UK GDPR and may include loss, damage, theft or disclosure to an unauthorised third party. In most cases a breach will result in a data subject suffering detriment, including a breach of their privacy and their expectations of how their personal information will be handled, as well financial or other tangible loss.
Complaints about the handling personal data can be made by any person whose information is held by the College and will be dealt with under the Complaints Policy and Procedure, with the advice of the Information Compliance team. Staff who believe their personal data may have been handled inappropriately can report this to their Line Manager, direct to the Information Compliance team, or can refer to the Grievance Policy and Procedure.

A member of staff who believes that there may have been an incident or breach or is in receipt of a complaint, must notify their Line Manager.

Managers who are advised of an incident, breach or complaint, must notify the Information Compliance team and complete a Personal Data Incident Report. The Information Compliance team will assist with an investigation of the matter, make recommendations for action and rectification, and will assess and advise whether a breach of the relevant legislation has occurred. The UK GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (ICO). This must be completed within 72 hours of becoming aware of the breach, where feasible, and in consultation with the Principal/Governing Body.

Where it is suspected that the actions/conduct of a member of staff has led to a breach of the UK GDPR, or other related legislation, consideration will be given to whether the matter should be dealt with under the Disciplinary Policy. Depending on the severity of the breach, the conduct may fall under the definition of Gross Misconduct outlined in that Policy.

Staff who have intentionally or negligently ignored any College policy, procedure or training related to the handling of personal data may be subject to a criminal investigation and proceedings.

Personal Data Incident Management Guidance Note.
To help support staff with potential Personal Data Incidents there exists a guidance note available to all staff via the Communications tab. This document sets out the process for managing and risk assessing incidents where personal data has been compromised, or where there is potential for it to be compromised. This document also provides staff with a blank Personal Data Incident Report template, which is also available as an separate editable PDF under the Communications tab.

6.19 Records Management

Records, including those containing personal information are subject to the Records Management Policy and Records Retention Schedule both published under the Communications tab. It is important to ensure that information, particularly personal information, is stored and logged in such a way that it can be located and retrieved at a later date, is required for business reasons, and in order to comply with legal requirements such as responding to a Right to Access or Freedom of Information request.

The College is responsible for the secure and accessible storage of records locally, and for ensuring their secure disposal at the appropriate time.

The Information Compliance team oversees the arrangements for records stored in commercial off-site storage.

Requests for the retrieval of archived personal files are subject to a protocol and when required, confirmation of the request by a manager.

6.20 Secure Storage and Handling of Personal Data

As well as the general guidelines issued under induction and core training, all staff receive training on appropriate local security arrangements for the type of personal data they will handle in the course of their role. This will include arrangements for:

- clear desk practice
- suitable secure storage
- locking screens when unattended, and the siting of screens/use of screen filters so information is not visible to others
- permission-based electronic storage
- secure sharing and transmission of information, using secure networks, cloud-based sharing, and encryption tools
- issue of College owned mobile devices equipped with appropriate encryption facilities. No personal data belonging to the College may be stored on personally owned mobile devices.

For more information about the security of information, please refer to the Information Security Policy published under the Communications tab or contact IT Services or the Information Compliance Team.

6.21 Disposal of Personal Data

Personal data held in hard copy form is disposed of as confidential waste using the appropriate bins/sacks and in accordance with the Disposal of Confidential Waste Guidance Note and related local arrangements.

The disposal of hardware that may contain personal data in a digital form is carried out by IT Services in accordance with the Information Security Policy.

6.22 Room and Building Re-assignments

Moving work locations introduces the risk of incidents where personal data is mishandled, either transported insecurely, lost in transit, left behind, or disposed of inappropriately. Managers and staff are responsible for ensuring that hard copy personal data stored in a staffroom, classroom or office which is under their remit, and which is to be vacated, is appropriately managed and prepared for transfer, including:

- personal data is to be transported in sealed boxes labelled with the owner and destination
- a sweep is to be made of the vacated room, including in, under and behind any cupboards, cabinets etc
- any personal information is disposed of securely (see 6.21).

Organisations may establish their own local procedures for ensuring room/building moves are managed correctly.

6.23 Staff Leavers/Transfers to new role

When an existing member of staff leaves or transfers to a new role within the College, the Line Manager is responsible for ensuring that relevant personal data (hard copy and digital) prepared and held by the staff member is accounted for. The personal data must be re-allocated to a new responsible person, be stored in an appropriate shared access area or is archived or destroyed as appropriate to the circumstances.

When a member of staff leaves the organisation, the Staff Leaver procedure is invoked by HR Services.

Staff leaving the organisation must not retain or copy any personal data belonging to the College. Staff are required to surrender Staff ID cards, door keys and cards giving access to secure areas as well as any issued IT equipment.

Managers must ensure that, particularly when a staff member moves to another role within the College, their access to any systems, databases, shared data storage areas and physical locations is revoked and reset as required.

6.24 Use of Email

Email as a means of communication is particularly vulnerable to information breaches where emails containing personal data are:

- sent to a wrong recipient,
- sent over non-secure internet connections, or
- contain information (often in a chain of emails) that is not appropriate for all recipients.

Depending on the sensitivity of the data (personal or otherwise) being transmitted via email, measures should be taken to protect the content, including anonymising (e.g. replace full names with initials), password protecting attachments, and using encryption tools.

Further information is available in the Handling Email Guidance Note available under the Communications tab.

6.25 Use of Office 365 (O365)

Office 365 offers an alternative storage and sharing solution compared to more traditional services.

Rather than sharing data via email, such as an attachment, staff can now consider sharing the same data via a secure link either via Sharepoint (internally) or OneDrive (externally). This works well if several members of staff are required to make amendments, or to simply view a document.

An advantage of sharing an O365 secure link is that the sender can manage access levels as well as having a better oversight of audit controls. O365 can also help limit the number of copies 'versions' of a document being circulated as multiple users can collaborate on (or view) the same document.

Although O365 does provide a great level of protection in many areas, consideration should still be given to whether any added protections are still needed to reduce any risk further. In many ways we would consider the same measures as we do with the use of email.

Further information is available in the Handling Email Guidance Note available under the Communications tab on the college homepage.

6.26 Use of Fax

Fax as a means of communication is particularly vulnerable to information breaches because of the risk of inputting an incorrect number and lack of awareness of the location of the receiving fax machine, which may be in an open office or shared between offices, departments and even businesses.

As a general rule Fax is not used to communicate personal information. However, if deemed necessary in cases of sufficient weight and urgency (and only where encryption/password protection for email is not available), it may be used but measures should be taken to minimise the risk, including:

- contacting the recipient to confirm the fax number
- double checking the input of the number is correct
- checking with the recipient the location of the receiving machine and arranging for the recipient to be at the receiving machine when transmission occurs
- checking with the recipient that the fax has been received in full.

6.27 Purchasing of Equipment or Software for Processing and Storing Personal Data

Before requesting or purchasing equipment or software for the storage and processing of personal data (e.g. mobile devices, surveillance equipment, internet-based services etc.), the College must consider any risks to privacy and consult with IT Services and the Information Compliance team for advice about security, encryption, and the suitability of the product for the purpose. The College will require systems and software products to incorporate the principle of 'privacy by design' to ensure they are fit for purpose under the UK GDPR.

6.28 Marketing

The UK GDPR provides individuals with the right to prevent processing of their personal data for direct marketing purposes.

Managers are responsible for ensuring that any marketing exercise in which they participate is undertaken lawfully and that the requirements of both the UK GDPR and the Privacy & Electronic Communications (EU Directive) Regulations 2003 are observed.

The Information Compliance Team can provide further advice covering:

- ensuring any marketing exercise is covered by the existing privacy notice and notification to the ICO, and arranging an update if necessary
- where the marketing involves data collected directly by the organisation, e.g. current student and/or parent details, they are notified of the intention to send them marketing information and given the opportunity to refuse their consent.

6.29 Contractors & Visitors

The conduct of contractors (particularly those that are not supervised) is covered in the Site Rules and includes requirements for confidentiality and compliance with data protection legislation. Visitors to and contractors working on sites belonging to the College are asked to notify Estates and Facilities should they have unauthorised access to personal data during the course of their visit/work, e.g. screens left unlocked, hard copy not put away.

Visitors and contractors are responsible for any personal data which they bring on to the premises.

7. Organisational Responsibilities

7.1 Governing Body / Principal & Senior Management

The governing body/board is the Data Controller for the College. The Data Controller has accountability for data protection and for ensuring that measures are in place relating to personal data being fairly, lawfully and securely processed.

The Data Controller has overall accountability for the strategic direction, oversight, monitoring, and leadership of data protection and is the named person responsible for ensuring that the objectives of the Data Protection Policy are achieved. This is designated to the Principal, Heads of Area and Department Managers.

The Data Controller is responsible for ensuring that the necessary resources are in place to secure full compliance with statutory requirements including the provision of appropriate technological and organsiational measures for the security of personal data and staff awareness training, and to ensure organisational arrangements are implemented effectively.

7.2 All Staff

All staff are responsible for:

- processing personal information fairly, lawfully and securely
- seeking guidance if they believe that personal data may be at risk of damage, loss or unauthorised disclosure
- reporting any incidents and/or breaches of the UK GDPR
- complying with all data protection requirements
- maintaining their knowledge and understanding of data protection, through regular mandatory training

All staff, whether or not they physically create, receive or maintain personal data themselves, have an obligation to comply with the principles and requirements of the UK GDPR.

7.3 The Information Compliance team

The Information Compliance team in the Governance and Legal Department have a central co-ordinating role in relation to general data protection matters, with particular emphasis on the provision of guidance and advice to the Data Controllers within the College relating to the requirements, interpretation and application of relevant legislation. Both the Data Protection Officer and the Director of Governance and Legal have a pivotal role in the development and promotion of the Data Protection Policy, strategic plans and, with the Executive Director of IT Services, the development of effective data protection security across the College.

The Data Protection Officer and Director of Governance and Legal fulfil the following functions:

- oversee the effective implementation of data protection legislation on behalf of the Data Controller
- provides competent advice and guidance to managers and other employees on matters of personal data
- reports to Data Controllers on data protection performance
- identifies and promotes relevant data protection compliance training for staff at all levels
- promotes a positive professional data protection compliance culture within the College in order to imbed privacy awareness as a norm in all personal data processing
- undertakes monitoring and auditing of data protection compliance across the College.

- develops opportunities for professional compliance shared services with external organisations.

7.4 Director of IT Services

The Executive Director of IT services is responsible for the management of security measures to protect personal data in all formats including electronic, images, and paper copy.

The Executive Director of IT Services will

- ensure that the appropriate technical measures are in place to protect personal data gathered, stored and transmitted via electronic means from unauthorised access and disclosure; and will provide advice and guidance on the appropriate level of physical security measures to protect personal data in other formats
- liaise with the Director of Governance and Legal and the Information Compliance team to ensure consistency of advice on information security measures and the content of training and awareness campaigns
- notify the Information Compliance Team of any projects, procurement and new processes involving personal data, and of any amendments or proposed changes to existing processing activities and assist with Data Protection Impact Assessment (DPIA).

8. Reference to other relevant policies and procedures

Policies, procedures and guidance

Policies
Information Security
Records Management
Social Media
Freedom of Information
Charging of Fees for the Provision of Information (Statutory Requests)

Procedures and Guidance
Record Retention Schedule
Disclosure of Personal Data and Request Handling
Use of Email
Use of Personal Images
Disposal of Confidential Waste
Student / Staff Conditions of Use of IT Systems
Room and Buildings Clearance
CCTV Code of Practice

9. Contact

For further information about any aspect of this policy contact in the first instance the Information Compliance Team on 01603 773585 / 3176 or email data_protection@ccn.ac.uk

10. Equal Opportunities Statement

This policy and procedure has been assessed against the nine protected characteristics outlined in the Equality Act 2010 and no apparent disadvantage to equal opportunities has been determined.

If you have any comments or suggestions in relation to equal opportunities of this policy or procedure please contact the policy holder.

Appendix 1 Relevant Legislation

General Data Protection Regulation (GDPR)

The GDPR (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

The GDPR details the statutory requirements for processing personal data. The Regulation includes the sanctions that apply in the event of a breach and misuse of personal information by individuals, including a criminal offence for disclosure of personal data which is unauthorised and carried out wilfully or negligently.

The GDPR is retained in domestic law now the Brexit transition period has ended, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018.

Data Protection Act 2018 (DPA 2018)

The Data Protection Act 2018 achieved Royal Assent on the 23rd May 2018. The 2018 Act modernises data protection laws in the UK to make the fit-for-purpose for our increasingly digital economy and society. The Act applies the EU's GDPR standards. Whereas the GDPR gives member states limited opportunities to make provisions for how it applies in their country, one element of the DPA 2018 is the details of these, applying as the national law.

Privacy & Electronic Communications (EC Directive) Regulations 2003

These regulations relate to direct marketing and make it unlawful to send someone direct marketing who has not previously given specific permission for their personal information to be used in this way (unless a previously existing relationship exists between the parties).
NB. There have been amendments to these regulations in 2004, 2011 and 2016.

Freedom of Information Act 2000 (FOI)

This statutory legislation places a requirement on all public bodies to manage records in such a way as to ensure that information is retained only as long as necessary and in such a way that it is identifiable and retrievable. The Act also allows any person to request any information held by a public authority. It is important to note that the Act applies only to certain parts the College; more information is available in the FOI Policy.

Protection of Freedoms Act 2012

The Protection of Freedoms Act:

- places a requirement on Data Controllers in Schools and Colleges to obtain parental consent for the gathering of biometric data.
- Regulates the use of CCTV for surveillance purposes.

Computer Misuse Act 1990

The purpose of this legislation is to secure computer material against unauthorised access or modification and for connected purposes; hacking and the introduction of viruses are criminal offences under this legislation.

Investigatory Powers Act 2016

This legislation limits and sets out circumstances in which individuals can be subjected to various forms of covert surveillance including telephone tapping, interception of correspondence and covert filming e.g. use of CCTV.

It specifically provides that the interception of private communications is unlawful other than where interception takes place in accordance with the provisions of the Act.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This legislation permits a business to intercept communications on its own network for business purposes and to detect email and internet abuse and to record telephone conversations to evidence transactions.

Education Specific Legislation and Statutory Guidance

There is a variety of legislation which creates either explicit or implied legal powers to collect, use and share personal data. (NB. this list is not exhaustive).

The Children Act (various dates)
The Education Act (various dates)
Education & Skills Act
Various Department for Education Statutory Guidance

Appendix 2 Data Protection Impact Assessment (DPIA)

A: Data Protection Impact Assessment (DPIA) Screening

It is important that City College Norwich (CCN) actively manages the risks around the processing of personal data. Part of this management is the completion of Data Protection Impact Assessments (DPIAs). These assessments encourage people to look carefully at what they are doing with personal data, why they are doing it, the risks involved and controlling those risks to an acceptable level.

Before you complete a DPIA, let's identify if one is required. If you answer YES to any of the questions below, please proceed to part B.

An editable (Word version) of the DPIA is available via the Communications tab or upon request from the Information Compliance team.

Screening Questions (please answer ALL questions)	YES/NO
Does your proposal involve the processing of any of the following? • CCTV • Biometrics (e.g. fingerprint, retina scan) • 'High Risk data' (see Annex D)	
Will the project/activity involve the collection of new personal information about individuals? (i.e. types of data the institution has not previously recorded, or about a group of individuals not previously involved)	
Will the project/activity require individuals to provide information about themselves? (i.e. will individuals have a **choice** of whether or not to provide the information?)	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? (This will include partnership arrangements with another organisation, requests from local authority/government agencies, providing data for a software service hosted online or by a third party)	
Does the project/activity involve you using new technology that might be perceived as being privacy intrusive? (For example, the use of biometrics, moving an existing process online, filming/recording individuals)	
Will the project/activity involve using data to make automated decisions or undertake profiling about individuals in ways that have a significant impact on them? (For example, using performance data to decide on salary increases)	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? (For example, 'special category data' such as health records, criminal records or other information that people would consider to be private?)	
Is data being transferred outside of Europe?	

B: Data Protection Impact Assessment (DPIA) Form

This form helps gather initial information internally, and from third party data processors with whom the organisation may need to share personal data for the fulfilment of a service. The form should be completed prior to a change in personal data processing OR the purchase of the service that involves the sharing of personal data. The form can also be used to assess a current service. If you have any questions regarding the completion of this form, please contact the Information Compliance team.

All sections can be expanded as required and the list of questions is not exhaustive. Responses may prompt additional enquiries. A completed copy of this document should be returned to the Information Compliance team (data_protection@ccn.ac.uk).

Document control information	
Service name:	
Date:	
Author(s):	
Service Contact point (for future privacy concerns)	

Step 1: Identify the need for a DPIA
Explain broadly what the project aims to achieve and what type of personal data processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal.
What does the project/service aim to achieve?
What are the expected benefits to the organisation?
What benefits to individuals and other parties are expected, if applicable?
Why was the need for a DPIA identified? (Refer to the Screening Questions)
What alternative solutions to the proposed project/service have been considered?
Why were these alternatives deemed unsuitable?

Note: Identify who is likely to be affected
This can include students, staff, parents/family members, staff from external organisations (e.g. partner agencies, contractors), the public.
The age of students can be a factor, and also mental capacity to understand their rights and how the proposed activity might affect their rights. Children, young adults, and individuals with impaired mental capacity are deemed to be more vulnerable to the impact of a breach of their privacy and personal data rights. In extreme cases, allowing unauthorised/inappropriate access to data can place a child or young adult at risk of physical harm.

Step 2: Describe the processing
Will the personal information be new information as opposed to existing information used in new ways?
Who are the Data Subjects? (Students, Staff, Contractors, Visitors, groups of these etc)
How many Data Subject records will be processed? (How many individual's records per year – is this cumulative?)
What types of data will be processed? (Name, Identifier, Address, Ethnicity, Images etc.)
Are all these data types required for the project/service?
Is the data adequate, relevant and not excessive? Can you minimise the amount of data being provided and still achieve the same outcome?
Is there a statutory requirement to process this data? (Please quote the regulations if 'yes')
How will you help to support the rights of the Data Subject(s)? (Right to access, right to be forgotten etc.)
What is the lawful basis for processing – Is the consent of the Data Subject required? (see GDPR Legal Basis for Processing Guidance Note)

Will the project/service involve new elements that require the organisation's Privacy Notice to be amended? If yes, please identify the changes that need to be made to the Privacy Notice.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Who should be consulted **internally** to help identify and address privacy risks?

The Information Compliance Team should be consulted in all cases.

(Roles / Groups):

Student Representative(s)	☐	IT Services (Security)	☐
Staff Representative(s)	☐	Procurement	☐
Governors	☐	Human Resources	☐

Other: Please specify

How will you consult internally?

Who should be consulted **externally** to help identify and address privacy risks?

The Information Compliance Team should be consulted in all cases.

(Roles / Groups):

Service Providers	☐
Contractors	☐

Other: Please specify

How will you consult externally?

Step 4: Identify and assess risks

Based on your responses to the screening questions and the three 'about' steps, identify the key privacy risks and the associated compliance and organisational risks. Depending on the scale of your project, you might also record this information on a more formal risk register. *Some example risks are listed at Annex A. To assist with determining the 'Overall risk', annexes B and E should also be consulted.*

Privacy issue	**Risk to individuals**	**Likelihood of harm:** ***Unlikely (1) Possible (2) Likely (3) Highly Likely (4) Almost Certain (5)***	**Severity of harm:** ***Minor (1) Moderate (2) Serious (3) Major (4) Severe (5)***	**Overall risk** ***Low, medium or high***	**Compliance risk**	**Associated organisation risk**
e.g. Security of data in transit between school and Service Provider	*e.g. Data subjects may be at risk of fraud, identity theft if data is not secured during transfer between school/individual and Service Provider*	*Possible*	*Moderate*	*Medium*	*e.g. Breach of data protection legislation*	*e.g. The ICO may require action, issue a monetary penalty if data is lost or misused*

Step 5: Identify measures to reduce risk Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance, training & awareness or future security testing for systems). *Some example measures are listed at Annex C.*			
Risk to individuals	**Measures to reduce or eliminate risk**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
e.g. Security of data in transit between school and Service Provider	*Set up private shared Onedrive folder for data drops and encourage schools to use this when sending data. All data received from individuals to be input within short timeframe and paper/electronic copies destroyed immediately after.*	*Reduced*	*Yes*

Step 6: Sign off and record the DPIA outcomes Who has approved the privacy risks involved in the project? What solutions need to be implemented? Further information: Read p. 30-31 of ICO Code of Practice		
Risk	**Approved solution**	**Approved by**
e.g. Security of data in transit between school and Service Provider	*Encourage schools to use OneDrive folder, and implement other appropriate security measures*	*Principal*

Review the Assessment and Update if Necessary

Risk assessments should be reviewed periodically to ensure that nothing has changed and that the control measures are effective.
Triggers for review may also apply if:

- Significant change has occurred e.g. further data is to be collected/used.
- The supplier changes or is using a new sub-contractor
- An incident or near miss has occurred.

Annex A – Examples of individual, organisational and compliance risks

Example Risks to Individuals

- Inappropriate disclosure of personal data internally within your organisation due to a lack of appropriate controls being in place.
- Accidental loss of electronic equipment by organisation's personnel may lead to risk of disclosure of personal information to third parties.
- Breach of data held electronically by "hackers".
- Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.
- Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen are not to be effective.
- Personal data being used in a manner not anticipated by Data Subjects due to an evolution in the nature of the project.
- Personal data being used for purposes not expected by Data Subjects due to failure to explain effectively how their data would be used.
- Personal data being used for automated decision making may be seen as excessively intrusive.
- Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.
- Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
- Use of technology capable of making visual or audio recordings may be unacceptably intrusive.
- Collection of data containing identifiers may prevent users from using a service anonymously.
- Data may be kept longer than required in the absence of appropriate policies.
- Data unnecessary for the project may be collected if appropriate policies are not in place, leading to unnecessary risks.
- Data may be transferred to countries with inadequate data protection regimes.

Organisational Risks

- Failure to comply with the UK GDPR may result in investigation, administrative fines, prosecution, or other sanctions. Failure to adequately conduct a DPIA where appropriate can itself be a breach of the UK GDPR.
- Data breaches or failure to live up to staff/parent/student expectations regarding privacy and personal data is likely to cause reputational risk.
- Public distrust of your organisation's use of personal information may lead to a reluctance on the part of individuals to deal with your organisation.
- Problems with project design identified late in the design process, or after completion, may be expensive and cumbersome to fix.
- Failure to manage how your organisation keeps and uses information can lead to inefficient duplication, or the expensive collection and storage of unnecessary information. Unnecessary processing and retention of information can also leave you at risk of non-compliance with the UK GDPR.
- Any harm caused to individuals by reason of mishandling of personal data may lead to claims for compensation against your organisation. Under the UK GDPR you may also be liable for non-material damage.

Compliance Risks

- Your organisation may face risks of prosecution, significant financial penalties, or reputational damage if you fail to comply with the UK GDPR. Individuals affected by a breach of the UK GDPR can seek compensation for both material and non-material damage.
- Failure to carry out a DPIA where appropriate is itself a breach of the legislation, as well as a lost opportunity to identify and mitigate against the future compliance risks a new project may bring.

Annex B - Evaluation of risk

Initially, it's important to consider the risk associated with the privacy impact without any control measures in place. The matrix on the assessment form at Annex E helps quantify the risks.

	L - Likelihood	S - Severity
5	Almost Certain	Severe
4	Highly Likely	Major
3	Likely	Serious
2	Possible	Moderate
1	Unlikely	Minor

The **Risk (R)** is determined by multiplying the **Likelihood (L)** with the **Severity (S) = (R = L x S).**

Risk	Values	Notes
Low Risk	1 to 7	
Medium Risk	8 to 15	
High Risk	16 to 25	Do not proceed, consult with the Governance and Legal department

Worked Example

Purchasing a subscription to an online software product – Student email address is provided to the software company to create user accounts and students access and to use the software online with user activity recorded.

Demographic data, e.g., Age, SEND status and financial support information is provided to create reports.

The principal privacy impact is:

- Student personal information being passed to an external third party, and the
- Data being stored outside the control of the College and
- Security arrangements are unknown.

Risk rating with no controls**: Likelihood - 3 (Likely)** multiplied by **Severity - 3 (Serious). R (Risk Rating) is 3 x 3 = 9 Medium Risk.**

The control measures to reduce the risk could be, assessing the third party for standards of security, putting a written and legally binding agreement in place, notifying students of the use, providing advice to students on keeping safe when online.

The residual risk rating could now be calculated as follows: **Likelihood - 1 (Unlikely)** *changed***,** but the **Severity - 3 (Serious)** does not change. The risk rating with controls would now be reduced to **1 x 3 = 3 Low risk.**

Annex C – Example measures to reduce risk

Every project will have its own unique circumstances and risk profile, so there is no “one size fits all” set of data privacy solutions which may be adopted. However, the following are examples of data protection measures, some of which may be applied in a range of different scenarios:

- Deciding not to collect or store particular types of information.
- Putting in place strict retention periods, designed to minimise the length of time that personal data is retained.
- Reviewing physical and/or IT security in your organisation or for a particular project team and making appropriate improvements where necessary.
- Conducting general or project-specific training to ensure that personal data is handled securely.
- Creating protocols for information handling within the project, and ensuring that all relevant staff are trained in operating under the protocol.
- Producing guidance for staff as reference point in the event of any uncertainty relating to the handling of information.
- Assessing the need for new IT systems to safely process and store the data, and providing staff with training in any new system adopted.
- Assessing the portability of using anonymised or pseudonymised data as part of the project to reduce identification risks, and developing an appropriate anonymisation protocol if the use of anonymised data is suitable.
- Ensuring that individuals are fully informed about how their information will be used.
- Providing a contact point for individuals to raise any concerns they may have with your organisation.
- If you are using external data processors, selecting appropriately experienced data processors and putting in place legal arrangements to ensure compliance with data protection legislation.
- Deciding not to proceed with a particular element of a project if the data privacy risks associated with it are inescapable and the benefits expected from this part of the project cannot justify those risks.

In most cases, there are some data protection risks which cannot be eliminated or reduced. These risks can be accepted if they are proportionate to the outcomes that will be achieved by proceeding with the project notwithstanding the risk. Any decisions to accept data protection risks should be recorded in the college risk register or sub-register such as a data protection risk register in accordance with college risk management process.

At this stage, you should also ensure that the project will be in compliance with data protection laws. In particular, you should consider whether the project complies with the data protection principles, and ensuring that you have a good legal basis for processing personal data.

Annex D – Special Category or ‘High Risk data’

Special category data is more sensitive, and so needs more protection. For example, information about an individual’s:

race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation. (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/)

Annex E - DPIA Risk Matrix

The tables below provide information regarding **Likelihood (L), Severity (S), Risk Rating (R),** and are for assessing the level or degree of risk. **L** is an assessment of the **Likelihood** of the hazard/privacy impact taking place, the second **S** for the **Severity** of the hazard/privacy impact, both based on the following:

	L - Likelihood	**S - Severity**
5	Almost Certain	Severe
4	Highly Likely	Major
3	Likely	Serious
2	Possible	Moderate
1	Unlikely	Minor

R is for the level of **Risk** which should be determined from inputting the **L** and **S** score into the risk matrix below. The aim is to reduce the risk by prevention or control measures so far as is reasonably practicable.

Risk Assessment Matrix:

S - Severity	**Extremely high**	5	5	10	15	20	25
	High	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	No Impact	1	1	2	3	4	5
			1	2	3	4	5
			Rare	**Unlikely**	**Possible**	**Likely**	**Almost certain**
			L - Likelihood				

Explanatory Note:

Risk:		**Likelihood:**	
20-25	High: Do not proceed, consult the Governance & Legal Department	**Almost certain**	Likely to occur
16-25	High: Do not proceed, consult the consult the Governance & Legal Department	**Highly likely**	More likely than not to occur
8-15	Medium	**Likely**	Has the potential to occur
1-7	Low	**Possible**	Unlikely to occur There is a possibility that it could occur
		Unlikely	Occurrence is extremely unlikely
Severity:			
Severe	• Multiple Fatality • Group-wide regulatory or legal action with irrecoverable financial and reputational consequences • Substantial and unwarranted damage or distress caused to multiple individuals		
Major	• Fatality • Organisation-wide regulatory or legal action with substantial financial and reputational consequences • Substantial and unwarranted damage or distress caused to an individual		
Serious	• Serious injury – reportable incident under RIDDOR such as fracture of bones, dislocation, amputation, occupational diseases (e.g. asthma, dermatitis), loss of sight • Institution subject to regulatory enforcement action with moderate financial and reputational consequences • Minor damage or distress caused to an individual		
Moderate	• Minor injury - First aid administered. Includes minor, cuts, bruising, abrasions and strains or sprains of ligaments, tendons, muscles • Institution subject to complaint requiring internal inquiry		
Minor	• Near Miss – no injury, no data loss.		

Annex F – Examples of Low, Medium and High Risk Personal Data

Personal Data – Sensitive (Special Category):	
Information of identifiable individuals': • Medical/health (incl. disability related risk assessments/adjustments) • Race/Ethnicity • Religious & other similar beliefs • Sexual Life • TU membership • Biometric • Genetic • Political affiliations/opinions • Commission/allegations of unlawful act (incl. outcomes)	**High**
Personal Data – Confidential:	
Information of identifiable individuals which could cause substantial unwarranted damage or distress, e.g.: • Set of identification details with the potential for fraud/identity theft (usually name, address, DOB, can include NI No, bank details, payroll no.) • Images of children/young people (with or without names) • Pastoral/HR records of conduct/behaviour, family circumstances, appraisal/performance record with personalised feedback/comment, allegations/investigations/outcomes of a disciplinary/performance nature, grievances	**High**
Personal Data:	
All other information of identifiable individuals, e.g.: • Student work, assessments, target/predicted grades, progression, grades/results • Courses/study programmes undertaken/enrolled in and dates • Employer sponsorship, funding, placements • Career history, role profiles, attendance, salary/payroll/expenses, • Next of kin/parent names & contact nos.	**Medium**
Personal Data - Work/study address information:	
• Work/student email address • Work telephone number • Work location & address • Work job title	**Low**