Governance and Legal Services

Data Protection Policy

NOTTINGHAM TRENT UNIVERSITY | 50 Shakespeare Street, Nottingham, NG1 4FQ

NOTTINGHAM TRENT UNIVERSITY

Version Control

Document Reference:	GDPR001
Policy Owner:	Governance and Legal Services
Approval Committee:	University Executive Team (UET)
Version:	Version 1
Next Review Date:	May 2019

Policy History

Version:	Author:	Reason for Issue:	Date:
Version 1	Legal Services	New Policy – including GDPR	23 April 2018

Contents

1. Introduction

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018 and it will replace the current Data Protection Act 1998. The GDPR intends to create consistency and strengthen data protection principles and practices across the EU. GDPR will apply to the entire UK despite the prospective outcomes of the UK leaving the European Union.

The GDPR administers a more up to date law on data protection, with stronger emphasis placed on the rights of individuals and how their personal data is used within organisations.

There are still many concepts which are the same with the redundant Data Protection Act but with new elements, particularly regarding data subject rights, accountability and organisational compliance with the GDPR Regulation's principles.

Nottingham Trent University (NTU) is committed to protecting the privacy and security of personal information which includes the personal data of our staff, students and other third parties. This Data Protection Policy sets out the minimum standards which must be complied with by NTU.

2. Scope

This Policy sets out how NTU (which includes Confetti Constellations Ltd, Nottingham Conference Centre Ltd, Nottingham Consultants Ltd, Nottingham Law School Legal Advice Centre Ltd, Nova Centric Ltd and NTU Temporary Staff Ltd) ("we", "our" or "us") identifies and manages its Data Protection responsibilities in accordance with its legal and regulatory obligations.

It is important for staff and students of the University ("you", "your") to understand the scope of the data protection legislation to enable us to comply with the legislation. This Policy sets out your responsibilities in relation to the data protection legislation, and applies to the entirety of NTU employees (including PhD students who are also employed by NTU), students and where appropriate third parties working for, or on behalf of NTU. It is your responsibility to familiarise yourself with this Policy which explains how you should carry out your job/role or research activity to ensure compliance with the data protection legislation.

3. Regulatory Requirements

This Policy has been documented giving consideration to, and in compliance with the following regulatory requirements.

Body	Regulation	Section / Paragraph
General Data Protection Regulation **(GDPR)**	Regulation	All
Information Commissioner's Office **(ICO)**	UK Independent Body/ Guidance	GDPR and FOI
The Freedom of Information Act **(FOI)** 2000	Regulation	All

Scope of the data protection legislation

The GDPR applies to the "Processing" of "Personal Data" wholly or partly by automated means (electronically) and to the processing other than by automated means where Personal Data form, or are intended to form, part of a filing system.

We have explained what this means in more detail below.

What is "Personal Data"?

Personal Data, or personal information, means any information about an individual from which that person (a "Data Subject") can be identified. It does not include data where the identity has been removed (anonymous data).The information will be Personal Data if a person can be identified either directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. For example personal data may include names, addresses, email addresses and telephone numbers; it may also include images in photographs or films and recorded telephone conversations.

We use Personal Data in relation to various types of Data Subject, including employees, students, potential students and applicants, business contacts, suppliers and contractors. There are special categories of Personal Data to which additional safeguards apply. This means special category Personal Data needs to be treated even more carefully than Personal Data.

These special categories of Personal Data include information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

What does "Processing" Personal Data mean?

The data protection legislation only applies to the "Processing" of Personal Data.

Processing has a broad definition and includes almost anything we might do with Personal Data, including obtaining, recording, organising, structuring, holding, storing, using, disclosing and destroying Personal Data.

It is difficult to think of anything we do with Personal Data that is not "Processing" it.

Who is the "Data Controller and "Data Processor"?

A "Data Controller" determines the purposes for which and the manner in which Personal Data is processed. For example, NTU is a Data Controller in respect of Personal Data we hold about you. NTU is also a Data Controller in respect of Personal Data we hold relating to students (e.g. their course details, their contact details, their educational record etc) and also the Personal Data we held about NTU's Alumni.

A "Data Processor" is any person who processes data on behalf of the Data Controller. A third party processing data on our behalf, as part of a service to NTU, is a "Data Processor". We are required to put in place a written contract with any Data Processors we use, to make sure that they reach the same high standards of data protection as NTU. NTU, as the Data Controller will remain responsible for the use of any Personal Data that it passes to any Data Processor.

Anyone wishing to appoint a Data Processor, or is concerned that they are passing Personal Data or Special Category Data onto a third party (i.e. a person or entity outside of NTU), should speak to the Legal Services Team to ensure that the arrangements being made are lawful.

While you are carrying out your role at NTU, you will not be classed as a Data Processor. However, if you act outside of your contract or role, you may become a Data Controller or Data Processor, and the legal obligations that fall to NTU as Data Controller could equally

apply to you. You could also expose both yourself and NTU to fines and/or a claim for damages from the Data Subject if you have used Personal Data in a way that was incompatible with the data protection legislation.

This is another reason why it is really important for you to be aware of the importance of data protection.

If you have any concerns about this, please let the Legal Services Team know.

4. Responsibilities

The University Executive Team (UET) has overall responsibility to ensure NTU meets its legal and regulatory responsibilities under GDPR, and to ensure compliance with this Policy.

We all use personal data in order to do our day to day jobs (for example to pay staff and to interact with and teach our students or to undertake research). It is important that the way we use (or "process") that personal data is compliant with the GDPR effective from 25 May 2018, together with the data protection legislation.

Some parts of the data protection legislation can sound quite technical and legal, particularly as a result of the various legal definitions and phrases that are used. We have therefore included a "Definitions of key terms used in this Policy" section to this Policy (page 16-18) and any questions or concerns about the interpretation or operation of this Policy should be addressed to the Legal Services Team in the first instance.

We also have a Data Protection Officer (DPO), who oversees all data protection issues. This is Tracy Landon, Legal Services Manager and Data Protection Officer DPO@ntu.ac.uk.

Key Points of this Policy

You must contact the **Legal Services Team** in the following circumstances:

- If unsure of the lawful basis upon which you are processing Personal Data (including the legitimate interests used by NTU);
- If you believe NTU's Privacy Notices are incorrect (our main privacy notices are available;
- If unsure about the retention period for the Personal Data being processed;
- If unsure about what security or other measures necessary to adequately protect Personal Data (see pages 10-11 on information security);
- If there has been an actual or suspected Personal Data Breach – Please see the Breach Notification Policy & Procedure;
- If there is a need to transfer Personal Data outside the European Economic Area as this is restricted unless specific legal conditions are met;
- If a request from a data subject to invoke their rights has been received (see page 13);
- Whenever engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment (DPIA) or plan to use Personal Data for purposes other than what it was collected for;
- If planning to undertake any activities involving automated processing including profiling or automated decision-making; and/or
- If wishing to enter into contracts or other activities involving sharing Personal Data with third parties (including our students and suppliers).

5. The Data Protection Principles

Anyone processing personal data on behalf of the University must comply with the six principles of GDPR in order to be legally compliant with the Regulation. Personal data must be:

1. Processed lawfully, fairly and in a transparent manner *(Lawfulness, Fairness and Transparency)*;
2. Collected only for specified, explicit and legitimate purposes *(Purpose Limitation)*;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed *(Data Minimisation)*;
4. Accurate and where necessary kept up to date *(Accuracy)*;
5. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed *(Storage Limitation)*; and
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage *(Security, Integrity and Confidentiality)*.

We have explained these in more detail below as it is really important that you understand how these principles work in order to ensure NTU's compliance with the legislation and to make sure that you do not breach this.

5.1 Lawfulness, Fairness and Transparency

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

The GDPR only allows Processing for specific purposes. These are known as the lawful grounds of processing or the conditions of processing. You need to comply with one of these grounds to make the Processing lawful and in compliance with the data protection legislation. The most relevant are set out below:

- The Data Subject has given his or her Consent; or
- The Processing is necessary for the performance of a contract with the Data Subject; or
- To meet our legal compliance obligations; or
- To protect the Data Subject's vital interests; or
- To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. NTU can only rely on legitimate interests when we are not carrying out a task as a public authority. This means we can only rely on "legitimate interests" in limited circumstances as the majority of what we do as a University are tasks carried out as a public authority. In the limited circumstances where we may be able to rely on legitimate interests, the purposes for which we process Personal Data must to be set out in applicable Privacy Notices.

We have to identify at least one of the above legal grounds and document which one(s) we are relying on for each Processing activity (i.e. each bit of Processing that we do).
If we cannot identify one of these legal grounds, we should not be doing that Processing.

Consent

Consent is one of the legal grounds that we can rely on when we Process Personal Data. What is meant by "consent" is defined in the GDPR. It needs to be a clear indication of agreement either by a statement or positive action to the Processing by the Data Subject. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient.

If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw their Consent to Processing at any time. Any withdrawal must be promptly acted upon. Consent may need to be refreshed (i.e. updated) on a regular basis. In addition, the Consent will need to be refreshed if NTU intends to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first gave their Consent. This means that if we collected a student's Personal Data and we relied on their consent to do various things (i.e. processing activities with that Personal Data), if we then want to do other or different things with their Personal Data using consent as the legal ground, we cannot rely on the "old" Consent. We would either need their new and updated Consent or to find another legal ground to process their Personal Data.

NTU will need to evidence any Consent that it relies on and retain a record of all Consents so that we can demonstrate that we have obtained the right Consent for the right processing activities. This is part of the accountability principle.

Transparency (notifying data subjects)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes or from students, we must provide the Data Subject (eg you or the student) with all the information required by the GDPR. This is contained in a document called a Privacy Notice and it is also described as a Fair Processing Notice. The two terms are sometimes used interchangeably.

Our Privacy Notices sets out this information out in relation to your employment/ engagement with NTU. We have to provide a different Privacy Notice to other categories of Data Subject, such as our students.

The Privacy Notice must include the identity of the Data Controller (i.e. NTU) and our DPO. It also sets out information such as how and why we will use, Process, disclose, protect and retain that Personal Data.

It is important that the Privacy Notice is given at the right time - when the Data Subject first provides the Personal Data to NTU.

When Personal Data is collected indirectly (for example, from a third party or publically available source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the Personal Data. We must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which considers our proposed Processing of that Personal Data i.e. that the individual knew that their Personal Data was going to be passed to us and for what purposed.

This means that all the third parties that we work with who Process Personal Data collected by NTU should also comply with the GDPR.

5.2 Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

We cannot use Personal Data for new, different or incompatible purposes from those disclosed to the Data Subject when it was first obtained.

This means if we collect Personal Data for one purpose, we shouldn't then use it for another purpose unless we tell the Data Subject what we are going to do and we have a legal ground to undertake that Processing.

5.3 Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only collect Personal Data that you require for your job role and duties: do not collect excessive data. You may only Process Personal Data when performing your job role requires it. You cannot Process Personal Data for any reason unrelated to your job role. You should ensure any Personal Data collected is adequate and relevant for the intended purposes. You shouldn't be collecting any field of Personal Data that is not necessary to the reason you are collecting it.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention guidelines. Please refer to our Data Retention Schedule for further information about how long we keep certain records for. It is also important that any records are destroyed and/ or deleted in accordance with our Data Retention Schedule, as safe and secure destruction is also required to comply with the data protection legislation.

5.4 Accuracy

Personal Data must be accurate and, where necessary, kept up-to-date. It must be corrected or deleted without delay when inaccurate.

NTU must ensure that the Personal Data we use and hold is accurate, complete, kept up-to-date and relevant to the purpose for which we collected it. NTU must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. NTU must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

5.5 Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

NTU must not keep Personal Data in a form where the Data Subject could be identified for longer than needed for the purpose or purposes for which we originally collected it (including for the purpose of satisfying any legal, accounting or reporting requirements).

We will maintain the Data Retention Schedule to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with our Data Retention Policy.

NTU must ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

5.6 Security Integrity and Confidentiality

Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

You are responsible for helping NTU protect the Personal Data we hold. You must comply with NTU's security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Category Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. These include IS Security Policies, Information Classification Policy, Cloud Security Policy and Guidelines, and the Data Retention Schedule which can be found on eCentral. In addition there are several guidance documents and FAQs on the Information Governance webpages.

If you fail to comply with NTU's security measures (either intentionally or inadvertently), this could lead to disciplinary action against you. This reflects the importance of keeping Personal Data secure.

NTU may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested. This is to make sure that those third parties adhere to NTU's high standards in relation to the security of Personal Data.

If you are transferring Personal Data to a third party, or if you want to transfer Personal Data to a third party, and you are in any doubt as to whether there is a lawful basis or appropriate contract in place, you should speak to the Legal Services team before transferring the Personal Data.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it. This means if you have access to Personal Data but it is not part of your job or role to access or Process such Personal Data, you should not do so.
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes. This means that you should not access or use any Personal Data if you are not permitted to.

You must comply with, and not attempt to circumvent, the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

Some of the safeguards we have in place to protect your Personal Data, students' Personal Data and other categories of Personal Data include:

- Access restrictions to internal systems;
- Card Access Building Security across the University;
- Encrypted portals for data transfer and password protection facilities;
- Unique user and password issued to each individual at NTU; and
- Secure remote access to internal systems.

Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable Regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects and/or any applicable regulator where we are legally required to do so. This can be found in the Data Breach Policy.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately notify the point of contact for Personal Data Breaches, which is the DPO. Their contact details are: **DPO@ntu.ac.uk**

You should preserve all evidence relating to the potential Personal Data Breach, including, but not limited to, emails or other correspondence, logs or screen shots, and complete the breach form with as much detail as possible.

If you fail to report a Personal Data breach in accordance with the Data Breach Policy, this could lead to disciplinary action against you. Compliance with this policy is critical to ensure that any Personal Data breach is dealt with carefully and promptly to protect the Personal Data of Data Subjects.

6. Transfer limitation

Data sharing

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of NTU (which includes our subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions (see the section on International transfers below for more information on this).

You may only share the Personal Data we hold with third parties, such as our service providers if:

- They have a need to know the information for the purposes of providing the contracted services;
- Sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains GDPR approved third party clauses has been obtained (or another lawful basis has been identified and approved).

As above, if you are transferring Personal Data to a third party, or if you want to transfer Personal Data to a third party, and you are concerned that there may not be an appropriate contract in place or are uncertain as to the legal basis upon which the Personal Data is being transferred, you should speak to the Legal Services Team by contacting DPO@ntu.ac.uk.

International transfers

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

NTU may only transfer Personal Data outside the EEA if one of the following conditions applies:

- Appropriate safeguards are in place, such as: binding corporate rules (BCR); standard contractual clauses approved by the European Commission; an approved code of conduct; or a certification mechanism applies; or
- The Data Subject has provided Consent to the proposed transfer after being informed of any potential risks; or
- The transfer is necessary for one of the other reasons set out in the GDPR, including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

If you are transferring Personal Data outside of the EEA or if you want to transfer Personal Data outside the EEA, and you are concerned that there may not be an appropriate legal arrangement in place, you should speak to the Legal Services Team to ensure that an appropriate legal arrangement is in place.

7. Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data.
These include rights to:

- Withdraw Consent to Processing at any time;
- Receive certain information about the Data Controller's Processing activities;
- Request access to their Personal Data that we hold;
- Prevent our use of their Personal Data for direct marketing purposes;
- Ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- Restrict Processing in specific circumstances;
- Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- Request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- Make a complaint to the supervisory authority; and
- In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

NTU must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the Legal Services Team and comply with NTU's Data Subject Access Request Policy.

8. Accountability

The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

This means that we must have adequate resources and controls in place to ensure and to document GDPR compliance including:

- Appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;
- Implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
- Integrating data protection into internal documents including this Data Protection Policy, Privacy Notices or Fair Processing Notices;
- Regularly training you on the GDPR, this Data Protection Policy, and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. We must maintain a record of training attendance by NTU staff; and
- Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

9. Record Keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities. NTU must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

9.1 Training and audit

We are required to ensure that all employees, workers, contractors, agency workers, consultants, directors, members and other individuals who work for and/ or are employed by NTU have undergone adequate training to enable them to comply with the data protection legislation. We must also regularly test our systems and processes to assess compliance.

Staff must undertake all mandatory data privacy related training, which is available online, and ensure members of your team undergo similar mandatory training in accordance with our training guidelines.

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

9.2 Privacy By Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles.

NTU must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

- The state of the art, the cost of implementation;
- The nature, scope, context and purposes of Processing; and
- The risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.
- NTU should conduct a DPIA when implementing major system or business change programs involving the Processing of Personal Data including:
- Use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Large scale Processing of Sensitive Data; and
- Large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- A description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
- An assessment of the necessity and proportionality of the Processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

If you are responsible for the implementation or management of a new project that may require a DPIA, you should speak to the Legal Services Manager in the first instance to ascertain whether a DPIA should be undertaken. If a DPIA is required, you must ensure that this is completed, with the assistance of the DPO/Legal Services Team.

10. Direct marketing

We are subject to certain rules and privacy laws when marketing to our students, our alumni and other Data Subjects.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing students known as "soft opt in" allows us to send marketing texts or emails if we have obtained contact details in the course of that individual undertaking a course at the University, we are marketing similar products or services, and we gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly acted upon. If a student, alumni member or other Data Subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

NTU should not undertake direct marketing to any individual who is not an existing student or has an existing commercial relationship with NTU without their Consent.

If you undertake direct marketing as part of your role, you must also familiarise yourself with the Marketing Data Use Procedure and the Direct Marketing Unsubscribe Procedure.

11. Definitions of key terms used in this Policy

There are lots of terms in this Data Protection Policy which come from the data protection legislation. The following terms have the following meaning:

You: all employees, workers, contractors, agency workers, consultants, directors, members and other individuals who work for and/ or are employed by NTU.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to you and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

GDPR: the General Data Protection Regulation ((EU) 2016/679)). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information relating to an identified or identifiable natural, living, person (Data Subject). An identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices (also referred to as Fair Processing Notices): separate notices setting out information that may be provided to Data Subjects when NTU collects

information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

12. Changes to this Data Protection Policy

We reserve the right to change this Data Protection Policy at any time so please check back regularly to obtain the latest copy of this Data Protection Policy. We will notify you when we update this Policy.

13. Escalation and Penalties

Breaching the GDPR can lead to fines and/or claims for compensation. There is also a reputational risk of negative publicity for NTU and risks to our other colleagues and students. For these reasons, if you fail to comply with the requirements of this policy, you may be subject to disciplinary action.

Data breaches must be notified to the ICO within 72 hours of the breach incident (when the breach happens). There is also a requirement to inform the data subject where the breach poses a high risk to their rights and freedoms.

Violations regarding record-keeping, security, breach notification, and privacy impact assessment obligations, can result in a penalty of up to €10 million or 2% of global gross revenue, whichever is greater.

More serious violations related to lawful processing of personal data such as consent, data subject rights and cross-border data transfers, can result in a penalty of up to €20 million or 4% of global gross revenue.

Please see the Breach Notification Policy and Breach Notification Procedure.