Polisi Safon Preifatrwydd

Privacy Standard Policy

Author: Catherine Lewis, Vice Principal: Corporate Services
Date May 2018
Version: Final

Contents

Section 1 : Introduction

1:01 NPTC Group of Colleges ('the Group') needs to keep certain information about its staff, students and other Group users for the purposes of:-

- monitoring performance;
- monitoring achievements;
- compliance with health & safety;
- employment of staff;
- curriculum provision;
- statutory compliance with funding bodies, the Welsh Government and the European Union.

1:02 To ensure compliance with current legislation, information must be:-

- collected safely;
- used fairly;
- stored safely;
- not disclosed unlawfully to other persons.

1:03 To this end, the Group will comply with the Principles for Processing Personal Data as set out in the EU General Data Protection Regulations (GDPR). Staff and others who process or use personal information, must ensure that personal data shall:-

- Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
- Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
- Accurate and where necessary kept up to date (Accuracy).
- 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).
- 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).
- Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
- Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

1:04 The Group and all staff or others who process or use personal information, must adhere to these Principles at all times.

1:05 The Freedom of Information Act 2000, gives a general right of access to all recorded information held by public authorities. However, the Act also identifies exemptions including information on staff and learners by virtue of it being personal information.

Section 2 : Status

2:01 This policy supersedes any previously approved Data Protection Policy. It was approved by the Group's Senior Management Team on 16.05.18, the Joint Information and Consultative Committee (JICC) meeting held on 16.05.18 and the Corporation Board on 24.05.18.

2:02 This policy has undergone Equality and Linguistic Impact Assessment and is attached as an appendix.

Section 3 : Policy

3:01 The Group will comply with the requirements of GDPR and, in particular, the Principles for Processing Personal Data (refer summary in Paragraph 1:03).

3:02 In addition to fulfilling its statutory obligation to comply with GDPR, the Group does so in the interests of openness, transparency and accountability, as defined by the Nolan Principles.

3:03 For the avoidance of doubt, this policy applies to all of the Group's, students, staff and wider users.

3:04 It is important to recognise that infringement of the legislation by staff or students may expose the Group and the individual to legal action and potential claims for substantial damages. Any infringement of the legislation therefore will be treated seriously and may result in action being taken under the terms of the Group's Disciplinary Procedures.

3:05 GDPR is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

3:06 For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in legislation. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data, as data controllers in the course of our business, we will ensure that those requirements are met.

Section 4 : Definitions

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Group: Neath Port Talbot College known as NPTC Group of Colleges.

Group Staff: all employees, workers, contractors, agency workers, consultants, directors, members, governors and others.

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 our Staff 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.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Group data privacy team with responsibility for data protection compliance.

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

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (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 identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. 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 Guidelines: the Group's privacy guidelines provided to assist in interpreting and implementing this Privacy Standard and Related Policies are available on SharePoint.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Group 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.

Related Policies: the Group's policies, operating procedures or processes related to this Privacy Standard and designed to protect Personal Data are available on SharePoint.

Sensitive Personal Data: 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.

Section 5: Context

5:01 This Privacy Standard sets out how NPTC Group of Colleges ('the Group') handles the Personal Data of our students, employees, customers, suppliers, contractors and other third parties.

5:02 This Privacy Standard applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

5:03 This Privacy Standard applies to all Group staff ("you"). You must read, understand and comply with this Privacy Standard when Processing Personal Data on our behalf and attend training on its requirements. This Privacy Standard sets out what we expect from you in order for the Group to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Privacy Standard. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Privacy Standard may result in disciplinary action.

5:04 This Privacy Standard (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Protection Officer (DPO).

Section 6: SCOPE

6:01 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Group is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

6:02 All managers are responsible for ensuring all Group staff comply with this Privacy Standard and need to actively encourage all staff to implement appropriate practices, processes, controls and training to ensure such compliance.

6:03 The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines. Please refer to Section 18 for contact details.

6:04 Please contact the DPO with any questions about the operation of this Privacy Standard or the GDPR or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Group) (see paragraph *8:01* below);

(b) if you need to rely on Consent and/or need to capture Explicit Consent (see paragraph *8:02* below);

(c) if you need to draft Privacy Notices or Fair Processing Notices (see *paragraph 8.3* below);

(d) if you are unsure about the retention period for the Personal Data being Processed (see Section *12* below);

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see *paragraph 13.01* below);

(f) if there has been a Personal Data Breach (*paragraph 13:02* below);

(g) if you are unsure on what basis to transfer Personal Data outside the EEA (see *Section 14* below);

(h) if you need any assistance dealing with any rights invoked by a Data Subject (see *Section 15*);

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 16:05 below) or plan to use Personal Data for purposes others than what it was collected for;

(j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see *paragraph 16:06* below);

(k) If you need help complying with applicable law when carrying out direct marketing activities (see *paragraph 16:07* below); or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see *paragraph 16:08* below).

Section 7: Personal Data Protection Principles

7:01 We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) 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).

(f) 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).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

7:02 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

Section 8: Lawfulness, Fairness, Transparency

8:01 Lawfulness and Fairness

8:01:1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

8:01:2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

8:01:3 The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests;

(e) 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. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

8:01:4 You must identify and document the legal ground being relied on for each Processing activity in accordance with the Group's guidelines on Lawful Basis for Processing Personal Data.

8:02 CONSENT

8:02:1 A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

8:02:2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. 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.

8:02:3 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

8:02:4 Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

8:02:5 You will need to evidence Consent captured and keep records of all Consents so that the Group can demonstrate compliance with Consent requirements.

8.3 Transparency (Notifying Data Subjects)

8:03:1 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.

8:03:2 Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by

the GDPR including the identity of the Data Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Fair Processing Notice which must be presented when the Data Subject first provides the Personal Data..

8:03:3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

8:03:4 You must comply with the Group's guidelines on drafting Privacy Notices / Fair Processing Notices.

Section 9: Purpose Limitation

9:01 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.

9:02 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

Section 10: Data Minimisation

10:01 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

10:02 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

10:03 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

10:04 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Group's data retention guidelines.

Section 11: Accuracy

11:01 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

11:02 You will 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. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

Section 12: Storage Limitation

12:01 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

12:02 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

12:03 The Group will maintain retention policies and procedures 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 the Group's policy on Data Retention.

12:04 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Group's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

12:05 You will 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.

Section 13: Security Integrity and Confidentiality

13:01 Protecting Personal Data

13:01:1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

13:01:2 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 protecting the Personal Data we hold. You must implement reasonable and appropriate 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 Sensitive Personal Data from loss and unauthorised access, use or disclosure.

13:01:3 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. You 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.

13:01:4 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

13:01:5 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 standard to protect Personal Data.

13:02 Reporting A Personal Data Breach

13:02:1 The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

13:02:2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

13:02:3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches the DPO and follow their guidance. You should preserve all evidence relating to the potential Personal Data Breach.

Section 14: Transfer Limitation

14:01 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.

14:02 You may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) 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, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) 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.

14:03 You must comply with the Group's guidelines on cross border data transfers.

Section 15: Data Subject's Rights and Requests

15:01 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) 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;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) 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.

15:02 You 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).

15:03 You must immediately forward any Data Subject request you receive to the DPO and comply with the Group's Data Subject response process.

Section 16: Accountability

16:01 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.

16:02 The Group must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Privacy Standard, Related Policies, Privacy Guidelines, Privacy Notices or Fair Processing Notices;

(d) regularly training Group Staff on the GDPR, this Privacy Standard, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Group must maintain a record of training attendance by Group Staff; and

(e) 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.

16:03 Record Keeping

16:03:1 The GDPR requires us to keep full and accurate records of all our data Processing activities.

16:03:2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Group's Record Retention Policy and guidelines.

16:03:3 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.

16.04 Training and Audit

16:04:1 We are required to ensure all Group Staff have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

16:04:2 You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training in accordance with the Group's mandatory training guidelines.

16:04:3 You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

16:05 Privacy by Design and Data Protection Impact Assessment (DPIA)

16:05:1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

16:05:2 You 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:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data controllers must also conduct DPIAs in respect to high risk Processing.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

(e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(f) Automated Processing including profiling and ADM;

(g) large scale Processing of Sensitive Data; and

(h) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

(i) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(j) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(k) an assessment of the risk to individuals; and

(l) the risk mitigation measures in place and demonstration of compliance.

16:05:3 You must comply with the Group's guidelines on DPIA and Privacy by Design.

16:06 Automated Procession (Including Profiling) and Automated Decision-Making

16:06:1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

16:05:2 If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

16:06:3 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

16:06:4 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

16:06:5 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

16:06:6 Where you are involved in any data Processing activity that involves profiling or ADM, you must comply with the Group's guidelines on profiling or ADM.

16:07 Direct Marketing

16:07:1 We are subject to certain rules and privacy laws when marketing to our customers.

16:07:2 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 customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

16:07:3 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.

16:07:4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer 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.

16:07:5 You must comply with the Group's guidelines on direct marketing to customers.

16:08 Sharing Personal Data

16:08:1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

16:08:2 You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

16:08:3 You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) 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;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

16:08:4 You must comply with the Group's guidelines on sharing data with third parties.

Section 17: Changes To This Privacy Standard

17:01 We reserve the right to change this Privacy Standard at any time so please check back regularly to obtain the latest copy of this Privacy Standard.

17:02 This Privacy Standard does not override any applicable national data privacy laws and regulations in countries where the Group operates.

Section 18: Contacts

Data Controller	Catherine Lewis 01639 648003 Catherine.lewis@nptcgroup.ac.uk
Data Protection Officer	Susan Kirby 01639 6480138 data-protection-officer@nptcgroup.ac.uk
Information Commissioner's Office (ICO)	Website: www.ico.org.uk Helpline: 0303 123 1113

Section 19: Acknowledgement of Receipt and Review

I, [EMPLOYEE NAME], acknowledge that on [DATE], I received and read a copy of the Group's Privacy Standard Policy, dated [EDITION DATE]] and understand that I am responsible for knowing and abiding by its terms. I understand that the information in this Privacy Standard Policy is intended to help Group Staff work together effectively on assigned job responsibilities and assist in the use and protection of Personal Data. This Privacy Standard Policy does not set terms or conditions of employment or form part of an employment contract.

Signed ……..

Printed Name …….

Date ……..

Equality and Linguistic Impact Assessment & Screening Document

This document is used to record the assessment of whether or not a policy, practice or provision - or a change to them - will have a negative or positive impact on the equality of a protected characteristic or on the use of the Welsh Language.

Stage 1 – Initial Screening

Firstly consider what item is being assessed and what is its purpose?

Using the boxes below, provide a description of the policy, practice or provision being assessed with a short statement about what the item is intended to achieve (its aims and objectives) and who is affected, eg staff, students, parents/carers, partners, etc.

Description of item: Privacy Standard Policy
Aims & objectives: The purpose of the Privacy Standard Policy is to ensure that all Group data, in all formats, is processed and held in compliance with legal and regulatory requirement, including General Data Protection Regulations (GDPR) which comes into effect on 25.05.18.
Those affected – eg staff, students, parents, partners etc : This policy applies to all persons working for the Group or on its behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners.

Considering the item being assessed, use the boxes below to record your initial thoughts on the possible consequences for the nine protected characteristics and the use of the Welsh Language.

Protected Characteristic	**Potential impact positive or negative**
Sex Also called gender, means a man or a woman	Having screened the policy we are confident that there are no implications for any of the protected characteristics. There is, therefore, no need to carry out any further analysis/assessment.

Race Refers to the protected characteristic of Race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins	

Protected Characteristic	**Potential impact positive or negative**
Age Where this is referred to, it refers to a person belonging to a particular age (e.g. 32 year olds) or range of ages (e.g. 18 - 30 year olds).	
Gender Re-assignment The process of transitioning from one gender to another	
Sexual Orientation Whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes	
Religion & Belief Religion has the meaning usually given to it but belief includes religious and philosophical beliefs including lack of belief (e.g. Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition.	
Pregnancy & Maternity Pregnancy is when expecting a baby, Maternity refers to period after the birth	
Marriage & Civil Partnership Marriage - between same or opposite sex couples, Civil Partnership - between same sex couples	
Disability Any long term condition that effects day	

to day activity. Conditions include hearing, visually & physical impairment, learning disability, mental health, cancer, HIV & MS	

Welsh Language	**Potential impact positive or negative**
The Welsh Language (Wales) Measure 2011 establishes equal rights for Welsh speakers, based on the principles In Wales, the Welsh language should be treated no less favourably than the English language & persons in Wales should be able to live their lives through the medium of Welsh if they choose	
Explanation – if appropriate	
Priority Level: high/medium/low	

Stage 2 – Analysis

Based on the screening process above you will need to carry out analysis to verify your initial decision. Below you need to show what equality and linguistic analysis has been done on this item? List the evidence, data or sources used to analyse the impact of this item. (include any, data, reports, surveys or web links utilised in the process)

Protected Characteristics	**Data Source & Findings**
Sex	We will be monitoring how the policy and procedures work in practice and will take into account any relevant feedback or information at next review.

Race	
Disability	
Sexual Orientation	
Age	
Pregnancy & Maternity	
Marriage & Civil Partnership	
Religion & Belief	
Gender Re-assignment	
The Use of the Welsh Language	**Data Source & Findings**
Welsh	

Stage 3 – Engagement/Consultation & Assessment

Following your analysis, you now need to record how you have assessed the item and who was engaged in the process. How was an assessment of the equality and linguistic impact reached, who was involved in the decision?

Group impacted	**Nature of positive and/or negative impact or explanation for no identified impact**
Sex	
Race	
Disability	

Sexual Orientation	
Age	
Pregnancy & Maternity	
Marriage & Civil Partnership	
Religion & Belief	
Gender Re-assignment	
Welsh	

Stage 4 – Mitigation & Changes

Finally, detail what changes have been made or are scheduled for change following the assessment & engagement to reduce or eliminate any adverse impact?

Impact	**Possible change**	**Recommended & actioned**
Not applicable as no adverse impact anticipated.		

Statement of justification and mitigation where negative impact cannot be avoided
N/A

Record of Evidence

1. Consultation

What consultation has taken place? (state when and who with)

Consultation process	**Findings**

2. Publication

When will the E&LIA be published?

Date and method: Will be attached to the policy as an appendix.

3. Monitor & Review

How will this item be reviewed & monitored

Lead person or group responsible and review dates : When policy reviewed unless introduction of any new legislation in the interim. **Vice Principal: Corporate Services**

Checklist

- Has the alternative format statement been included at the start of the policy document?
  If you or someone you know would like this document in an alternative format please contact the HR Unit at hr@nptcgroup.ac.uk or on 01639 648308.

  Has the document been formatted in line with NPTC Group of Colleges publication guidelines and policy template?

- Has the Equality & Diversity paragraph been included at the end of section 1 for all policies?
  If any member of staff requires assistance with understanding or implementing this policy, particularly where the reasons for this are related to disability, religion or belief, sex, gender reassignment, sexual orientation, pregnancy or maternity, age or race they should contact the HR Unit, in the first instance for advice.

- When you have completed the paperwork please ensure it is added as an appendix to the relevant policy or procedure

- Any questions? please contact the HR Unit on 01639 648308 or by email hr@nptcgroup.ac.uk

Signature of Assessment Manager & other staff completing ELIA

Name (s) – please print

Catherine Lewis, Vice Principal: Corporate Services

Melanie Dunbar, HR Manager

Signature (s) Date 16.05.18