Norpro Training Ltd

Student Data Protection Policy

Introduction

Norpro Training Ltd, hereafter known as Norpro, needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Norpro must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Norpro and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, Norpro has developed this Data Protection Policy.

Status of the Policy

1. This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by Norpro from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.
2. Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller initially. If the matter is not resolved, it should be raised as a formal grievance.

Notification of Data Held and Processed

All staff, students and other users are entitled to know:

a. What information Norpro holds and processes about them and why.
b. How to gain access to it.
c. How to keep it up to date.
d. What Norpro is doing to comply with its obligations under the 1998 Act.

Norpro will therefore provide all staff and students and other relevant users with a standard form of notification. This will state all the types of data Norpro holds and processes about them, and the reasons for which it is processed, Norpro will endeavour to do this at least once every three years.

Responsibilities of Staff

All staff are responsible for:

a. Checking that any information that they provide to Norpro in connection with their employment is accurate and up to date.
b. Informing Norpro of any changes to information, which they have provided. I.e. changes of address.
c. Checking the information that Norpro will send out from time to time, giving details of information kept and processed about staff.
d. Informing Norpro of any errors or changes. Norpro cannot be held responsible for any errors unless the staff member has informed Norpro of them.
e. If and when, as part of their responsibilities, staff collect information about other people's (i.e. about student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff (see Staff Data Protection Policy).

Data Security

All staff are responsible for ensuring that:

a. Any personal data which they hold is kept securely.
b. Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
c. Staff should note that unauthorised disclosure and/or failure to adhere to the requirements set out in 5.3 to 5.7 inclusive below will usually be a disciplinary matter and may be considered gross misconduct in some cases.
d. Personal information should be;

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- if kept or in transit on portable media the files themselves must be password protected.

- Personal data should never be stored at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites.

e. Ordinarily, personal data should not be processed at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Head of School or Department must be obtained, and all the security guidelines given in this document must still be followed.
f. Data stored on portable electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment. It is the responsibility of this individual to ensure that:

- Suitable backups of the data exist.
- Sensitive data is appropriately encrypted.
- Sensitive data is not copied onto portable storage devices without first consulting the Head of School or Department, in regard to appropriate encryption and protection measures.
- Electronic devices such as laptops or PDA's, and computer media (floppy disks, USB devices, CD-ROM's etc…) that contain sensitive data ARE not left unattended when offsite.

g. For some information the risks of failure to provide adequate security may be so high that it should never be taken home. This might include payroll information, addresses of students and staff, disciplinary or appraisal records or bank account details. Exceptions to this may only be with the explicit agreement of the Principal.

Student obligations

Students must ensure that all personal data provided to Norpro is accurate and up to date. They must ensure that changes of address, etc are notified to the Course Administrator.

Students who use Norpro computer facilities may, from time to time, process personal data. If they do they must notify the data controller. Any student who requires further clarification about this should contact the Manager.

Rights to Access Information

Staff, students and other users of Norpro have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete Norpro "Request form for access to data" and give it to the Project Manager.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing. Norpro aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 40 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Publication of College Information

Information that is already in the public domain is exempt from the 1998 Act. It is Norpro policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Names and contacts of Norpro Directors.
- List of staff.
- Photographs of key staff.

Norpro's internal phone list will not be a public document. Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Project Manager.

Subject Consent

In many cases, Norpro can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to Norpro processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. Norpro has a duty under the Children Act and other enactments to ensure that staff members are suitable for the job, and students for the courses offered. Norpro also has a duty of care to all staff and students and must therefore make sure that employees and those who use Norpro facilities do not pose a threat or danger to other users.

Norpro will also ask for information about particular health needs, such as allergies, particular forms of medication or any conditions such as asthma and diabetes. Norpro will only use the information in the protection of the health and safety of the individual but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff and students will be asked to sign a Consent to Process form, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race, gender and family details. This may be to ensure Norpro is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for Norpro to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the Project Manager.

The Data Controller and the Designated Data controllers

Norpro as a body corporate is the data controller under the Act, and the board is therefore ultimately responsible for implementation. However, there are designated data controllers who deal with day to day matters.

Norpro Training Ltd designated data controllers:

Stacey Rowe	Reception
Brian Weatherston	Technical Manager

Examination Marks

Students will be entitled to aggregated information about their marks for both coursework and examinations. However, this may take longer than other information to provide. Norpro may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned to Norpro.

Retention of Data

Norpro will keep some forms of information for longer than others, Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so, in general information about students will be kept for a maximum of ten years after they leave Norpro.

This will include:

- name and address,
- academic achievements, including marks for coursework and
- Copies of any reference written.

All other information, including any information about health, race or disciplinary matters will be destroyed within 7 years of the course ending and the student leaving Norpro.

Norpro will need to keep information about staff for longer periods of time; In general, all information will be kept for five years after a member of staff leaves Norpro. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. A full list of information with retention times is available from the data controller.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of Norpro. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated data controller.

Reviewed by Stacey Rowe Nov 2021
Next review Nov 2022