General Data Protection Regulation (GDPR) and Privacy Policy

This generally applies to where NPCL holds or collects data on individuals in an electronic format but also in the way we protect this printed information. It encompasses individual's digital rights to information and protection of the data our organisation collects or holds about them.

This information can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information or a computer's IP address. From time to time we are required to hold certain information about individuals for funding purposes – in such cases we will make individuals aware of the information we are collecting and often this will be in writing - example a signed enrolment form.

Your Personal Information

When you first enter NPCL premises we may create a personal information form with your name and details. Any information that you give us from then on may be added to this record.

NPCL is committed to the protection of your personal information in accordance with the principles of the Data Protection Act 1998 and GDPR 2014.

NPCL is registered with ICO (Information Commissioner's Office) under the Data Protection Act 1998 and GDPR which it renews yearly.

We can provide information of what we hold to the person in question. Please note that we cannot provide information about others; only information that we hold about the applicant.

NPCL hold all hardcopy information at a secure location and in a locked facility.

Use of your Personal Information

Your personal information is used in the following ways:
To be kept for Health and Safety reasons e.g. in the case of contacting next of kin. Your personal details may be passed onto our funders or partners (e.g. Lottery) on request e.g. in the case of an audit. We do not sell or give away your details to any other organisations.

With your prior permission we may publish certain details or images about you in social media, the Internet, local or national media.

We will use your details:
To process any application you make for membership or any courses that you apply for at NPCL and to maintain those details. We will use your details to process any application for additional services; such as learning, training, conferences or meetings. If your application is for an event that is sponsored, your contact details will be passed to the sponsor of the event. You will be informed if your details are to be passed to the sponsor when you apply to attend.

- To provide information about additional services that may be of interest to you.
- To undertake research in order to help us plan and improve our services.
- To provide information to funding bodies, e.g. The Lottery.

Length of retention:
NPCL will hold personal records for a minimum of 7 years and if linked to financial information or funded projects 7 years. For ESF based projects information will be held for a minimum of 12 years. All projects can be archived after 2 years. Boxes will be clearly marked with project name, summary of contents and date of destruction if information is to be destroyed.

Destruction of information after minimum retention period has expired:
The destruction of any materials of hardcopy containing personal data should be a cross shredder before burning, recycling or landfill. Please seek the permission of either the Chair or Charities Secretary. The summary of data destroyed should be kept on file and signed and dated by the Chair or Secretary.

Sending or sharing of electronic data:
If any personal data is to be transferred across the Internet that is more than is in the public domain permission may need to be sought. It is recommended that you follow the instructions under the **Email** heading latter in this policy and ensure that all personal information is sent securely email) the file containing the data be zipped and password protected to 15 characters; being a mix of letters, numbers and special characters and attached to the said email. A text or phone message to give the password to the intended party is expected, never from within the same email.

Please discuss with the Data Protection Coordinator if unsure of how or when to do this. Otherwise avoid sending confidential data via the Internet.

Email

When responding to emails all staff should be aware of the information contained therein, especially if it is of a personal nature e.g. date of birth/ national insurance number or medical information. If this is the case the email may be sent as an attachment in a zipped file that is encrypted and password protected the password being sent via Text, written or spoken form but NOT within the same email (**see passwords**). The data controller will be responsible for making such emails GPDR compliant BUT data processers must inform the data controller of the need.

Further:

- Staff not to use email to identify more than 10 customers/clients
- Only use the minimum necessary personal data for viewing, access or transference
- Identify sensitive personal data
- Transfer of sensitive personal data must be protected from loss by use of encrypted electronic methods (as mentioned above) or a monitored postal service e.g. Special Delivery Guaranteed
- Double check that information is being sent to the correct recipient
- Identify duplicate and redundant material

- Staff to utilise secure email methods for all emails relating to personal information of clients and this to be attached in an encrypted file with a password of 15 characters.

Posting of sensitive data

- Include return address on back of the envelope
- Never mark the classification on envelope
- Consider double envelope for highly sensitive assets (write the classification on the inner envelope only)
- Use registered Royal Mail service - Special Delivery Guaranteed

Printed Information

All personal details of individuals (including staff) will be kept in a locked filing cabinet/safe. It is the responsibility for all staff to keep a clean desk and ensure all/any printed personal information in the office or centre is kept securely locked in the office filing cabinet at the end of day and if staff are leaving the office, even to just visit the gardens or go toilet, it must be kept locked.

Display Boards

All information should be checked to ensure that it complies with data protection and is up to date anything that is not should be removed.

Website

Our website currently does not collect information other than if someone contacts us through email in which case they will be using their own email system. If we respond to them then we follow the guidelines below.

Data Collection

Pseudonymization will be employed by the data controller when collecting data for individual funded projects to make it less obvious for thieves, hackers or anyone else trying to obtain data we store on computers, cloud storage or by any other electronic means. Hence file names or data headings will not necessarily say what they mean e.g. the word passport might be represented by pp for example.

When databases are used they will be stored on a secure encrypted server, as will shared by trusted staff folders only e.g. DBS checked staff/teachers/trustees.

Information security (InfoSec)

This is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. NPCL will deploy various procedures through the data controller to enforce the above mentioned within the GPDR Policy.

We will have digital information stored on an encrypted server that is on a secure LAN and not a Wireless connection. This will be accessed by computers in the centre.

PEN drives and removable drives such as USB devices, writable DVD's are BANNED for company use in the centre computers without the express written permission of the data Controller and if they contain any private information including pictures/photos or data this should be encrypted so that should the device containing the data be lost it cannot be easily retrieved by a third party.

Passwords

As a back-up passwords shall be kept printed in a locked filing cabinet in a hidden manner (known to trustees and staff) and also requiring another code to access that is held in the second key cabinet in order to make extra secure.

Passwords shall be at least 12 characters in length and recommended 15 characters or more. Passwords should contain Capital and lowercase letters, numbers and special symbols where appropriate. Passwords should not be easily guessable and sent via text or another format different to the same email address in question. See the data controller for advice.

Lawful Basis for Processing

Data can only be processed if there is at least one lawful basis to do so. The lawful bases for processing data are:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes (e.g. signed enrolment form/signing in sheets with disclaimer on the bottom – ***"We may store your information on a database/or keep your files in a secure place onsite. We may share this information with our funders especially if you are on a course supported by them. We will not sell your information and we will comply with GDPR to ensure it is kept safe and secure. By using our services you are abiding to our GDPR and Privacy Policy and so are we".***
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- processing is necessary for compliance with a legal obligation to which the controller is subject.
- processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the

interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Data breaches

- Under the GDPR, the Data Controller will be under a legal obligation to notify the Supervisory Authority (ICO.org.uk) without undue delay. The reporting of a data breach is not subject to any de minimis standard and must be reported to the Supervisory Authority within 72 hours after having become aware of the data breach. Individuals have to be notified if adverse impact is determined. In addition, the data processor will have to notify the controller without undue delay after becoming aware of a personal data breach.
- However, the notice to data subjects is not required if the data controller has implemented appropriate technical and organizational protection measures that render the personal data unintelligible to any person who is not authorized to access it, such as encryption.

Individual Rights

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The right to be Informed

The data subject has given consent to the processing of his or her personal data for one or more specific purposes and the uses for the data e.g. marketing/funding are explained (e.g. signed enrolment form with disclaimer).

The right of access

The Right of Access is a data subject right. This gives citizens the right to get access to their personal data and information about how these personal data are being processed. A Data Controller has to provide, upon request, an overview of the categories of data that are being

processed as well as a copy of the actual data. Further more the Data Controller has to inform the data subject on details about the processing such as; what the purposes are of the processing, with whom the data are shared and how it acquired the data.

Individuals may request information we hold on them via the GPDR Information request form. Available from the office.

The right to rectification

Before any possible errors can be changed the person requesting the change should be confirmed as to whom they claim to be so as to avoid giving out or changing information about someone else.
This ID confirmation could be providing a photo ID like a passport/driving licence or that they are already know face to face by staff. A copy of this ID is not required.

Such information and changes needed should be checked by the data controller and not just the data processor.

Right to Erasure

Provided that the data subject has the right to request erasure of personal data related to them on any one of a number of grounds including non-compliance (lawfulness) that includes a case where the legitimate interests of the controller is overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. In some cases a funder may need to be contacted first.

The right to restrict processing

While we are able to do this e.g. someone does not wish to give their Date of Birth, DOB but we are able to record name and address; in some cases of funding if certain information is not collected then the person may have to pay in full in order to attend the course as otherwise they will be outside of the funding parameters set by the funder.

Data Portability

A person shall be able to transfer their personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller. Data that has been sufficiently anonymised is excluded, but data that have only been de-identified but remains possible to link to the individual in question, such as by him or her providing the relevant identifier, is not. Both data that have been 'provided' by the data subject, and data that have been 'observed' — such as about their behaviour — is within scope. In addition, the data must be provided by the controller in a structured and commonly used Open standard electronic format.

The right to object

Any person has the right to object to us collecting information; however we also have a care of duty to all those attending our centre and gardens and under certain circumstances such a

person may not be able to use certain facilities or provisions at the centre e.g. funded programmes that require certain information like postcode data in order for a person to receive free or reduced training fees or cases of employing staff and requiring a DBS check.

Rights in relation to automated decision making and profiling

Information is normally recorded as supplied by the individual however we will sometimes represent that information differently e.g. John Barnes may be J B in order to protect the individuals privacy even further. If individuals are concerned with the way we store their information they can make a request to the data controller whom will be happy to provide a print out of what information is recorded on them.

Data protection by Design and by Default

Data protection by Design and by Default requires that data protection is designed into the development of business processes for products and services. This requires that privacy settings must be set at a high level by default and that technical and procedural measures should be taken care by the controller in order to make sure that the processing, throughout the whole processing lifecycle, complies with the regulation. Controllers should also implement mechanisms to ensure that personal data are only processed when necessary for each specific purpose.

A report by ENISA (the European Union Agency for Network and Information Security) elaborates on what needs to be done to achieve privacy and data protection by default. It specifies that encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved. The report specifies that outsourced data storage on remote clouds is practical and relatively safe, as long as only the data owner, not the cloud service, holds the decryption keys.

Records of processing activities

Records of processing activities must be maintained, that include purposes of the processing, categories involved and envisaged time limits. These records must be made available to the supervisory authority on request.

Contact

If you have any comments or questions regarding this policy, please contact the Data Controller:

Data Controller

The data controller can be contacted through:

NPCL, Engage, St Levan Road, Plymouth, PL2 3BG
Email:info@npcl.org.uk Tel: 01752 551862
Web Site: http://www.npcl.org.uk

The data controller is responsible for the companies processing of personal data and can handle any individual requests for information held on the individuals making the request but not on the behalf of others without a signature from them on the data request form.

Data Processor

This is a person or persons employed by NPCL and under instruction of the Data Controller. All data Processors must be made aware of this policy and sign a form to agree to the terms of NPCL and this policy.

Supervisory Authority

Information Commissioner's Office (ICO)
www.ico.org.uk
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Telephone: 0303 123 1113 or 01625 545745 **Fax:** 01625 524510

Data Request Form

Please either post or email this form to the data controller.

We will do our best to answer your request within 14 working days.

PLEASE WRITE IN CAPITALS Date: _____

First Name _____ Surname: _____

Contact Details:

Address_____

_____

_____

Telephone Number: _____ Email: _____

Nature of request (please tick as needed):

Please send information that you hold on me: ☐

Please make the following amendments to information held on me:☐

*Please erase information you hold on me:☐

Other:

* This may incur a fee when funding has been gained due to a postcode area, employment or other information needed in order to gain reduced or free training with NPCL.

Applicants Signature_____

NPCL Signature_____Position_____

Date Received: _____