DIGITAL PENINSULA NETWORK LTD

(DPN)

DATA PROTECTION ACT AND POLICY (incorporating DPA 2018 & GDPR)

Author: Janus Howard Version: 13	*Policy reviewed annually:* Last reviewed January 2026 Next review January 2027
Signature: 	Date: 27th January 2026
Changes Made: pg 4 amended to 7 key principles pg 7 Title Change to Data Protection Officer Pg9 added para under Notification of Data request to external Data Controller.	

DATA PROTECTION ACT & POLICY

Purpose

The purpose of the Act is to protect the rights of the individual about whom data is obtained, stored, processed or supplied rather than those of the people or organisations who control and use personal data. The Data Protection Act 2018 and General Data Protection Regulation (GDPR) are technologically neutral, so this policy covers all manual records and data held electronically.

The Act requires that appropriate security measures will be taken against unauthorised access to, or alteration, disclosure or destruction of personal data and against accidental loss or destruction of personal data.

Definitions

"*Personal data*" is any information that relates to an individual who can be identified from that information.

"*Special categories of personal data*" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"*Processing*" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Scope

The 2018 Act applies to:

- Computerised personal data
- Personal data held in structured manual files

It applies to anything at all done to personal data ("processing"), including collection, use, disclosure, destruction and merely holding data.

Principles of Data Protection

The Act is based on seven key principles stating that data must be:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

The GDPR are in place to protect individuals by regulating the way in which DPN collects, retains and uses personal data. Storing and processing data is governed by specific principles which state that DPN shall:

- process personal data lawfully, fairly and in a transparent manner;
- collect personal data only for specified, explicit and legitimate purposes;
- process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing;
- keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- keep personal data only for the period necessary for processing in accordance with funder's guidance (such as Education and Skills Funding Agency);
- adopt appropriate measures to make sure that personal data is secure, and protected; against unauthorised or unlawful processing, and accidental loss, destruction or damage;
- implement organisational and technical measures to ensure and be able to demonstrate that processing is performed in accordance with the regulations.

How does it affect me?

Employees can also be prosecuted for unlawful action under the legislation. Fines could result if you use or disclose information about other people without their consent or proper authorisation. You could even be committing an offence if you give information to another employee, member or individual who does not need the details to carry out their legitimate duties.

You should take particular care when using the Internet, e-mail and the internal network. Special care must be taken with sensitive data such as ethnic origins, religious/political beliefs, health data, disabilities, details of offences or alleged offences, sexual life or trade union membership.

All staff and members have a duty to observe the Principles of the Act. Individuals who do not handle data as part of their normal work have a responsibility to ensure that any personal data they see or hear goes no further. This includes personal data and information extracted from such data, thus, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer screen.

General Guidelines

- Do not leave people's information on your desk when it is not in use,
- Lock all filing cabinets
- Do not leave data displayed on screen, do not leave your computer logged on and unattended
- Do not give your password to anyone under any circumstances
- Do not choose a password that's easy to guess

DPN Data Protection Policy

DPN needs to keep certain personal data, for example about its staff and members, to fulfil its purpose and to meet its legal obligations to funding bodies. 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, DPN must comply with the Data Protection Principles which are set out in the Data Protection Act, 2018 and General Data Protection Regulations 2018 (GDPR).

DPN takes seriously its obligations under Act, and we are registered with the Information Commissioner. Our registration, which is renewed annually, allows us to process certain personal information following very strict guidelines, which define the data subjects, the classes of data, which may be held, and the data recipients. For the purpose of the Act the nominated representative for Data Protection compliance is Managing Director, Janus Howard, Deputy is Senior Tutor, Sioban Osborne.

We hold data for the purposes of Staff Administration, Membership Administration, Training Administration, Contract Administration and realizing our objectives. Personal data is defined as 'information about a living individual who is identifiable by that information, or who could be identified by the information combined with other data; it includes recorded opinion about or intentions regarding a person'.

The data falls into two main categories:

1. **Staff data (DPN employees)**
2. **External data**

Staff Data

What?

Various data is held on staff relating to their employment with DPN. This will cover all aspects of recruitment, selection and employment such as

- Job application forms
- Interview assessments
- References
- Probationary and annual reviews and supervisions
- Bank details and national insurance number, details of any deductions from pay (e.g. to the courts…or to trades unions)
- Sick notes and medical assessments
- Details of grievance and disciplinary proceedings including current warnings (within the timescale allowed by the appropriate policies)
- Reference requests, etc.

Much of this data is, by its nature, highly personal, and DPN recognizes that it is its duty to safeguard the data by all possible means, and to notify staff about what is kept and why, along with information on how the data can be accessed and by whom.

Why?

The data kept on staff is exclusively in relation to their employment with DPN - no unrelated data will be kept. The data that is kept will be used for the purpose of administering and managing the employment.

Where?

Most personal data is kept in individual personnel files in a locked cupboard in the
DPN Centre. Other data (bank details, NI number, deductions details etc) are kept by the Financial Administrator, and these are kept locked.

Computer files (supervision records, payroll details etc) are password protected and secured.

Whom?

Access to staff data is restricted to

- The Managing Director
- The Financial Administrator for any issues specifically relating to pay
- and to administrative staff (in connection with file maintenance, employment correspondence and the like).

Staff are entitled to see their own personnel files - to do so, they should arrange a mutually convenient time with their manager / managing director.

Personal data held on computers (including files, emails, databases, etc) and personal data downloaded from the web or posted on the web are subject to the same control and restrictions as paper-based data. Staff must take particular care when using any personal data in these contexts.

Staff Obligations

While the Managing Director is the Registered Data Protection Officer, all staff are responsible for ensuring their compliance with this Policy. Misuse of personal data is a disciplinary offence, and may even constitute a criminal offence.

All staff and members are responsible for:

- Checking that any personal data that they provide to DPN is accurate and up to date and informing DPN of any changes to or errors in information which they have provided i.e. changes of address.
- Personal data which they hold is kept securely (files should be kept locked up, and computers should be password protected) and is disposed of safely.
- Personal information about another member / member of staff is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party, unless permission has been granted by that person

References

References may only be given by the Managing Director at DPN. Particular care must be taken when providing references, either employment-related or personal. Information relating to personal data (e.g. attendance records, discipline, etc) must not be provided without the express written consent of the data subject.

Data Storage Time

There are various statutory requirements regarding how long some types of data must be kept. For example, any data relating to health and safety (particularly if this is linked to staff records) must be kept for 40 years. Financial records have varying archive periods, usually of 6 years. Recruitment records are usually kept for 1 year and staff records for 7 years (unless these relate to health and safety – see
above).

Staff are encouraged to seek further information from the Managing Director if unsure about archive requirements, and are reminded that archive records must be kept locked at all times.

External Data

DPN recognises its duty to safeguard the data it holds on members, external groups and individuals. We have conducted an audit of all data held, disposed of outdated information, and arranged secure storage systems for current data including locked/password protected storage, and locked archive facilities.

In addition, the following steps have been taken:

- All written materials (membership packs, contracts, output forms, website, training data & evaluation forms, have been designed to ensure that all data is being kept with permission.
- DPN will not supply mailing lists or contact details from its member / client information unless the express consent of these members has been obtained first.

Notification of Data Held and Processed

Staff and members and other users of DPN have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. Any person who wishes to exercise this right should make the request in writing to the Managing Director, using a standard form which is available from the Managing Director or by emailing gdpr@digitalpeninsula.com

Where DPN is the sub-contractor and therefore Data Processor, the Managing Director will notify the relevant authority (Data Controller) of any requests/breaches of data protection.

DPN aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one calendar month of receipt of a completed form unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

All staff, members and other users are entitled to:

- Ask what information DPN holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed what DPN is doing to comply with its obligations under the Data Protection Act 2018.
- Request for DPN to rectify any inaccurate data / erase the data that the organisation hold about them

Other Relevant Policies

Various DPN Policies relate to and should be read alongside this Policy – for example:

- Disciplinary Procedure
- Equality and Diversity Policy
- DPN Complaints Procedure

Any questions or concerns about the implementation of this Policy should be addressed to the Managing Director, and further information on data protection issues generally are available from https://ico.org.uk/