Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

Policy Title:	**Data Protection Policy**
Policy Owner:	**Chief Legal Officer**
Implemented:	**March 2023 (updating May 2018 Data Protection Policy)**
Revision Date:	**November 2026**

DATA PROTECTION POLICY

Employees of the NEP Group ("**NEP**") are responsible for protecting NEP and employee information regardless of the medium.

For further information, please read the body of this document.

TABLE OF CONTENTS

PART A: NEP'S RESPONSIBILITIES TO YOU UNDER DATA PROTECTION LAWS 2
1. The type of information we collect about you 2
2. The manner in which we may process your Personal Data 2
3. With whom we share your Personal Data 4
4. Data transfers 4
5. Retention of records 5
6. Monitoring 5
7. Your data rights 6
PART B: YOUR RESPONSIBILITIES TO OTHERS UNDER DATA PROTECTION LAWS 6
8. Data privacy team 6
9. Data protection principles 7
10. Keeping data secure 7
11. Reporting suspected data security breaches 12
12. Ensure that Personal Data is accurate and kept up to date 12
13. Securely disposing of personal data 12
14. Privacy impact assessments 12
15. Training 13
16. Data protection and disciplinary action 13
17. Changes to this data protection policy 13

Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

EXPLANTATORY NOTE AND STATUS OF THIS POLICY:

NEP Group, inc. together with its subsidiaries (see www.nepgroup.com/contact-us) is referred to in this policy as "**NEP**"/ the "**Company/ies**" / "**we**"/ "**us**"/ "**our**". NEP needs to collect and process certain information about individuals in order to run its businesses effectively. This information comes from, amongst others, current, past and prospective employees, workers, job applicants, customers, accreditors, suppliers and other individuals with whom NEP communicates and does business.

However, in doing so we are responsible to these individuals for ensuring that we use their information with care and in compliance with privacy and data protection laws ("**Data Protection Laws**"). Our brand and organisational values require that we adopt and comply with good data governance procedures, including those which are set out in this Data Protection Policy ("**Policy**").

This Policy sets out (in Part A) how NEP will use its staff's data, and (in Part B) guidance as to some of the key measures which NEP expects its staff to take when it comes to NEP's data processing activities. This policy sets out our rules on data protection and the conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

PART A: NEP'S RESPONSIBILITIES TO YOU UNDER DATA PROTECTION LAWS

This notice ("**Notice**") describes the categories of personal information that the NEP entity you are employed or contracted by ("**NEP**", "**we**", "**us**" and "**our**") collects in relation to its employees, workers and contractors ("**employees**" and "**you**"), and the purposes for which that information is used. The controller of your Personal Data is the NEP entity that you are employed with or contracted by.

1. The type of information we collect about you

The types of Personal Data which NEP will process in the course of its engagements with you include:

- names, addresses, telephone numbers and other personal contact details;
- gender, date of birth, government issued numbers (e.g. national insurance number, national ID number, social security number), driver's license, immigration status, marital status, next of kin;
- personnel records including training, appraisal, resumes, performance and disciplinary information, and succession planning;
- bank details, salary, bonus, benefits and pension details;
- CCTV images and call recordings;
- Your use of our systems and provided hard- and software (also see section 6); and
- Travel history, copies of passports, copies of driving license, passwords and identifiers and VISA information.

2. The manner in which we may process your Personal Data

We only process your Personal Data where we have a legitimate purpose. NEP undertakes a number of activities with your Personal Data, depending on the entity that you are employed by these may include:

Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

Contractual obligations: for the performance of a contract or in order to take steps prior to entering into a contract with you.

- salary, benefits and pensions administration;
- managing your employment and your relationship with NEP; and
- criminal records checks, credit checks and clearances (where applicable).

Legal obligations: for compliance with a legal obligation to which we are subject.

- health and safety records and management;
- equal opportunities monitoring (insofar required by law);
- any potential change of control of a group company, or any potential transfer of employment relating to a business transfer or change of service provider (in Europe, under the Acquired Rights Directive). In such circumstances, Personal Data may only be disclosed to the potential purchaser or investor and their advisors to the extent permitted by applicable law; and
- compliance with applicable procedures, laws, regulations, including any related investigations to ensure compliance or of any potential breaches.

Legitimate interests: for the purposes of legitimate interests pursued by NEP or by third parties.

- establishing, exercising or defending NEP's legal rights;
- confirming information on resumes and covering letters, providing reference letters and performing reference checks;
- provision of staff information to customers and agencies in the course of the provision of NEP's services;
- CCTV monitoring for security reasons;
- equal opportunities monitoring;
- any potential change of control of a group company, or any potential transfer of employment relating to a business transfer or change of service provider (in Europe, under the Acquired Rights Directive). In such circumstances, Personal Data may only be disclosed to the potential purchaser or investor and their advisors to the extent permitted by applicable law;
- any other reasonable purposes in connection with an individual's employment or engagement by NEP;
- compliance with applicable procedures, laws, regulations, including any related investigations to ensure compliance or of any potential breaches;
- other disclosures required in the context of staff employment promoting or marketing of NEP, its products or services;
- operation of any ethics or whistleblowing hotline which NEP may run now;
- providing and managing use of services provided by third parties, such as company provided mobile phones, company credit cards and company cars and billing for such services; and
- training and appraisal, including performance evaluation and disciplinary records;
- staff management, salary decisions and promotions; and
- succession planning.

Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

In certain limited cases, we ask for your further specific consent to use your data. Whenever we ask for your consent we will explain the situations where we use your data and for what purposes.

NEP may also collect and process Personal Data about your next of kin so they can be contacted in an emergency or in connection with use of a company car provided by NEP. Their Personal Data will also be processed in accordance with the Data Protection Laws and as described in this Policy. Where NEP requires you to provide Personal Data about other individuals (including your next of kin), NEP relies on you to notify those individuals of our collection of their Personal Data and obtain their consent to their Personal Data being processed by us in accordance with the Data Protection Laws and as described in this Policy.

3. With whom we share your Personal Data

Sometimes we may need to share your personal information with other affiliated companies and third parties. We will only do so when this is necessary for the performance of the employment contract with you, for our legitimate business purposes or where permitted under law.

For example, your personal information may be shared with: (i) affiliated companies for the purposes of human resource administration; (ii) external suppliers to administer your benefits on our behalf, (iii) our advisers and insurers; (iv) our carefully selected service providers appointed from time to time to provide services related to our business and under contract to us, such as processors of employee data, salary, expenses and other compensation information; and (iv) external parties as required by law or legal process, or as otherwise authorised by you.

4. Data transfers

NEP may transfer Personal Data to other group companies, partners, suppliers, law enforcement agencies and to other organisations that are located outside of the European Economic Area ("**EEA**"), the UK or the jurisdiction that you are located in (for staff working outside the EEA) for the purposes of:

- HR administration (for example, staff recruitment and management);
- payroll processing;
- staff relocation;
- visa applications;
- taxation and registrations;
- fulfilling NEP's legal requirements;
- fulfilling customer contracts for the provision of NEP's services;
- overseas legal proceedings; and
- outsourcing NEP functions.

The countries to which Personal Data may be transferred may include, among others, the US (where NEP is headquartered and where a number of its service providers, e.g. Microsoft is located), the countries in which NEP has operations, and the location of suppliers and their data centres.

Where personal information of EU or UK employees is transferred outside the EEA or UK, and where this is to a NEP affiliate or supplier in a country that is not subject to an adequacy decision by a relevant body such as the European Commission, data is adequately protected by approved standard

Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

contractual clauses such as those approved by the European Commission or a vendor's Binding Corporate Rules.

If you are an employee located outside of the EEA and your personal information is transferred to another jurisdiction, NEP will put in place measures to ensure that such transfers take place in compliance with applicable local standards in the jurisdiction that you are located in.

NEP has put in place an intragroup data transfer agreement based on approved transfer mechanisms that enables and facilitates the transfer of personal information within the NEP group.

If you wish to hear more about these safeguards and how we apply them, please contact us through the contact details further below or reach out to your Regional Privacy Champion.

5. Retention of records

NEP has a statutory duty to keep certain records for a minimum period of time. NEP shall not keep Personal Data for longer than is necessary or as may be required by applicable law. For further information about NEP's approach to data retention contact your Regional Privacy Champion.

6. Monitoring

Monitoring of NEP's systems

For business reasons, and in order to maintain IT security measures, the use of NEP's systems on a relevant platform including the telephone (mobile and fixed) and computer systems (including email and internet access), and any personal use of them, may be monitored, if and to the extent permitted or as required by law and as necessary and justifiable for business purposes.

To the extent permitted by law and, where breaches of this Policy are found, action may be taken under the disciplinary procedure.

All equipment (computers and mobile telephones in particular) which NEP may put at the disposal of its staff in the course of their work for the company is for professional use only.

NEP reserves the right to retrieve the contents of messages, check searches which have been made on the internet, require the immediate return of devices supplied by NEP and access data stored on such devices for the following purposes:

- to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this Policy (and staff acknowledge that NEP can use software to monitor the identity of senders and receivers of emails);
- to find lost messages or to retrieve messages lost due to computer failure;
- to assist in the investigation of wrongful acts, including those in breach of our other policies or applicable law; and
- to comply with any legal obligation.

A condition of use of our IT systems is that you behave in a professional manner, do not bring the good name of the company into disrepute and do not behave in an inappropriate way in relation to your colleagues and others whom you contact using communications whilst working for NEP. If evidence of a breach of these conditions or of misuse of NEP's IT systems is found, NEP may undertake a more detailed investigation in accordance with NEP's disciplinary procedures, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the disciplinary procedure. Likewise, if NEP has a reasonable suspicion that illegal activity or actions which would breach our other policies and procedures has taken place.

Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

CCTV

Some of NEP's buildings and sites use CCTV systems to monitor their exterior and interior 24 hours a day for security reasons. This data is recorded and may be archived for viewing at a later time. Use of CCTV and recording of CCTV data is only carried in accordance with NEP approved guidelines.

7. Your data rights

Under Data Protection Laws you may be entitled to ask NEP for a copy of your Personal Data, to correct it, erase or restrict its processing, or to ask NEP to transfer some of this information to other organisations. You may also have rights to object to some processing of your Personal Data and where NEP has asked for your consent to process Personal Data, to withdraw this consent. These rights may be limited in some situations — for example, where NEP demonstrates that it has a legal requirement to process your data. In some instances, this may mean that it can retain data even if you withdraw your consent.

Where NEP requires Personal Data to comply with legal or contractual obligations, the provision of such data is mandatory: if such data is not provided, then NEP will not be able to manage the employment relationship, or to meet obligations placed on us. In all other cases, provision of requested Personal Data is optional.

Your information is not used in any automated decision making (a decision made solely by automated means without any human involvement) that produces legal effects or otherwise significantly affects you.

To exercise your data rights, to express your concerns or complaints or pose your questions about how NEP processes staff Personal Data, please contact your Regional Privacy Champion.

You have the right to complain directly to data protection authorities. The relevant data protection authority will be the supervisory authority in the same country as your employing entity.

PART B: YOUR RESPONSIBILITIES TO OTHERS UNDER DATA PROTECTION LAWS

8. Data privacy team

NEP has appointed a team of Regional Privacy Champions to help it comply with its obligations under Data Protection Laws. The key role of the Regional Privacy Champions is as follows:

- to provide a point of contact and support for staff;
- to carry out and support the carrying out of privacy impact assessments;
- to provide training to staff;
- to liaise with the local data protection authority; and
- to deal with information access requests and other data subject rights.

If having read this Policy or at any time you have any queries relating to the way in which you should handle Personal Data, then please contact your Regional Privacy Champion.

Your Regional Privacy Champion can be found here: (https://nepanywhere.oak.com/u/5EA8F785).

If you are unable to contact your Regional Privacy Champion for any reason, please contact Information Services or NEP Legal.

This part of the Policy is intended to inform staff about how they should handle Personal Data in certain circumstances. Each and every member of staff has an obligation to comply with Data Protection Laws. It is important that individuals are aware of their own data protection responsibilities

Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

towards others under Data Protection Laws, which include the need to follow the guidelines and processes set out below. Here are some key points to remember:

- Consider your responsibilities under Data Protection Laws and this Policy and how they impact on your day-to-day activities.
- Only share Personal Data (or commercially sensitive data) on a need-to-know basis. Don't share an entire database where only a part of it is needed.
- Double check the recipient's details before sharing data. Are you sending data as intended or putting the company at risk?
- Use password protection for documents and files, wherever appropriate.
- Only use Personal Data in the way that the individual concerned has agreed or as set out in this Policy.
- Take a common-sense approach when deciding how to protect, use and dispose of Personal Data. Think about how you would like your personal information to be treated.

This section is intended to provide general guidance and is not a comprehensive or exhaustive guide. Depending on the precise nature of your job, you may have additional responsibilities to others under Data Protection Laws.

9. Data protection principles

In processing any Personal Data NEP and its staff must adhere to certain data protection principles contained within the Data Protection Laws. These include that Personal Data must:

- be processed fairly and lawfully;
- be processed only for one or more specified and lawful purposes, and not further processed in any manner incompatible with such purposes unless expressly permitted under applicable laws;
- be adequate, relevant and not excessive in relation to the purposes for which they are processed;
- be accurate and, where necessary, kept up to date;
- be kept no longer than is necessary for the purposes for which it is processed;
- be processed in accordance with an individual's rights, including a right in certain circumstances: to access Personal Data, to have it ported to a third party, for it to be erased if inaccurate or no longer required and not to be subject to significant automated decision making processes;
- be kept secure; and
- only be transferred to or accessed from a country or territory outside the country or territory in which the Personal Data was collected, if that overseas country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of Personal Data or where adequate contractual safeguards to protect the data are in place.

10. Keeping data secure

The provisions of this section and section 4 (Reporting suspected data security breaches) relate not just to Personal Data but to all information, IT and communications systems. You are responsible for

Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this Policy.

Computer/laptop security:

- All IT users will have been given unique account details. You must not share accounts or passwords. You must not use accounts not assigned to you or disclose your account details to others.
- You should always lock, logoff or shut down your computer or laptop or handheld device during periods where you will be leaving them unattended (e.g. to attend meetings or during lunch breaks). NEP's IT systems are designed, where possible, to automatically lock or terminate after a designated period of inactivity.
- At the end of each working day, you should ensure that your computer is properly shutdown and that your monitor is switched off. If you have a laptop, it should be stored securely, for example in a locked cabinet or drawer.
- Ensure that business sensitive confidential information shown on a screen cannot be easily overseen.
- You must use a strong password (e.g. a mixture of capital and lower case letters, numbers and special characters) and keep it confidential. You should change it regularly and if you believe someone knows your password, you must change it immediately.
- Alterations to or maintenance of your computer or IT equipment or the installation of any hardware or software on NEP supported assets is to only be completed by NEP's Information Services team, its associates or authorised individuals with the expressed permission of the Information Services team.
- Immediately report a lost or stolen device such as a laptop or mobile phone, even if your phone is for personal use.
- Report any suspicious activity occurring on your computer that does not appear to be normal.

Access to data stored electronically:

- Use passwords to restrict access to sensitive files.
- Do not circumvent any established security groupings or authorisation levels.
- Keep an audit trail for amendments made to databases or documents containing sensitive information.
- Do not prevent any scheduled IT back-up processes.

Security of portable devices:

- If you have been given access to NEP supported IT systems or infrastructure, you are responsible for its safekeeping and for taking reasonable steps and care to ensure it is not used by unauthorised parties, lost, stolen or damaged especially when travelling or when you are outside of the office.
- Portable devices must not be left in vehicles at any time, particularly overnight, but if absolutely necessary, you should make sure that they are kept out of sight.
- If you are using portable devices on, for example, public transport or in a public place like a hotel foyer, you should ensure that the screen cannot be read by others, and you should take appropriate precautions in light of that risk.
- If you use your portable device on any external or third-party network, for example, at a hotel or airport, you should take reasonable steps to ensure that the network is secure, for example,

Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

by using a network provided by a reputable company and which is preferably password protected rather than available without restriction. If you have any doubts about the security of the network, you should not connect your device to it.

- You must not attempt to circumvent any encryption software or security features on the portable devices.
- NEP uses a combination of the following security features on portable devices to ensure that they are kept secure:
    - usernames/passwords and PIN numbers;
    - anti-virus protection;
    - data encryption;
    - account lock out following failed access attempts;
    - device/application lock following inactivity;
    - account or device lock out following theft/loss;
    - monitoring of use; and
    - deletion of content on lost or stolen devices.

On-site security of paper copies of Personal Data:

- Keep your desk clear of Personal Data and business sensitive confidential information.
- Do not leave Personal Data or business sensitive confidential information unattended on desks at any time.
- If you are printing sensitive Personal Data or business sensitive confidential information, then make sure you stand by the printer to collect it to avoid it being picked up by someone else.
- Do not leave Personal Data or business sensitive confidential information in meeting rooms or other areas of the office, take them with you and dispose of them securely if you no longer require them. Wipe white boards clean before leaving meetings rooms unless clearly instructed not to.
- Lock/store material containing Personal Data and business sensitive confidential information in a secure place overnight such as a lockable filing cabinet, drawer or in a restricted access or locked area/room.
- Follow any specific guidance relating to your location or department.

Off-site security of paper copies of Personal Data:

- Only take Personal Data or business sensitive confidential information outside the office or off-site if it is absolutely necessary.
- Be aware of the risks of loss or theft and take appropriate precautions to make sure Personal Data or business sensitive confidential information is kept secure.
- Do not leave Personal Data or business sensitive confidential information unattended at any time on trains or other forms of public transport or in other public places. Make sure that business sensitive information cannot easily be overseen when you are in a public place.
- Only store or archive Personal Data or business sensitive confidential information off-site using a NEP approved supplier with whom a written contract is in place.

Use of mobile storage media:

Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

Portable/removable media ("**Media**") includes any portable device capable of storing, transferring, manipulating or removing data and includes (but is not restricted to) mobile devices, flash disks/pens, removable hard drives and optical media (CDs, DVDs etc.).

- Data may only be transferred from NEP's IT systems to other Media where there is a genuine business justification and the provisions of this Policy and directions from the Information Services team are followed.
- NEP monitors all data copied from the network to detect unauthorised data transfer and prevent security breaches.
- The exchange of data either internally or with external parties should always be via NEP information systems such as email or shared data areas. Use of Media for data transfer should only be used when all other options have been exhausted.
- Any Media physically transferred between NEP and/or a customer should be sent by special delivery (to ensure that the Media can be tracked and recovered if lost).
- Before using Media, note:
    - You may only use Media that has been purchased through or authorised by NEP Information Services and encrypted;
    - Media should be capable of being tracked to ensure arrival at the intended destination;
    - Media must be scanned for malware/virus infection using virus scanning software provided by NEP's Information Services team prior to use and not used if found to carry a potential infection;
    - Only store data that is absolutely necessary, i.e. do not download an entire database if only small sections of it are required;
    - Check that the mobile storage Media can encrypt the Personal Data;
    - Ensure that files held on the Media are password protected with the password being sent separately to the encrypted Media;
    - Immediately delete data from the Media once it is no longer required; and
    - Non-reusable Media is to be correctly disposed/destroyed at the end of its required lifecycle in accordance with the Information Services team's recommendations.

<u>Restrictions on use of unauthorised devices or software</u>:

- Hardware that is not procured and/or managed by the Information Services team (e.g. personal or third-party laptops, tablets, smart phones, mobile phones, memory sticks etc.) cannot be connected to or installed on NEP equipment or networks without explicit permission from the Information Services team.
- You must not download unlicensed software, third party software, freely available software or any similar software onto your computer or other IT equipment because it may contain viruses or other malicious code that could breach the security of NEP's systems.

<u>Third-party access</u>:

- NEP is responsible for the acts and omissions of its suppliers and contractors who may access or process Personal Data on its behalf. If you are engaging contractors, consultants and temporary staff who have access to NEP's systems and/or Personal Data, they must first sign an agreement containing provisions that adequately protect NEP's Personal Data, for example, confidentiality and security. You should contact the head of HR or divisional Legal counsel for guidance on the provisions required.

Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

- In particular, any project involving the connection by a third party/supplier to NEP's systems will require a specific assessment of the risks and additional contractual terms relating to security.
- All changes to third party/supplier access to NEP's network must be reviewed and documented to ensure that security is maintained.
- If third party/contractor access is no longer required, connectivity must be terminated and any Personal Data obtained by the third party/contractor returned or destroyed in accordance with the contractual terms.
- All third-party suppliers and contractors must be required to notify NEP, via their primary point of contact, of all information security incidents experienced by themselves or their customers.

Back-up Data:

- Wherever possible data should be held in networked storage as this can easily be backed up using automated processes. Removable media such as USB flash drives and CDs should not be used for storing business critical information as it will not be backed up and therefore will not be recoverable if lost, corrupted or accidentally deleted.

Disposal of Personal Data:

Personal Data in paper form must be disposed of using confidential waste bins or by using paper shredders. If a confidential waste bin is not available, please contact the designated facilities manager at the specific site/location/building for collection arrangements.

- Ensure any IT hardware, mobile devices, mobile storage media or other equipment is properly cleansed of all Personal Data before disposal. Non-reusable media such as CD-ROMs must be correctly disposed of or destroyed at the end of its required lifecycle. Contact the Information Services team to ensure this is carried out correctly.

Email and system use:

- You must not attempt to circumvent virus protection software for example by disabling it.
- Employees should exercise caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious (for example, if its name ends in .exe).
- The Information Services team should be informed immediately if a suspected virus is received or identified or a link in an email has been clicked prompting you to disclose personal information.
- NEP reserves the right to block access to attachments to e-mails for the purpose of effective use of NEP's IT systems and for compliance with this Policy.
- NEP also reserves the right not to transmit (in-bound or out-bound) any e-mail message if a virus is suspected to be attached.
- NEP permits the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and NEP reserves the right to withdraw permission at any time. NEP reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers personal use to be excessive. The following conditions must be met for personal usage to continue:
    - use must be minimal and take place substantially out of normal working hours;
    - use must not interfere with business or office commitments; and

Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

- use must not commit NEP to any marginal costs.

- The use of webmail sites (such as Hotmail, Yahoo and Gmail) to send or receive business related information is forbidden unless there is a genuine business justification which is approved by the Information Services team. All email traffic related to business activities must be through an approved corporate email system.

Customer contact details:

- You must not leave any hard copy address books or other documents or devices containing business contacts unattended.
- If you store business contacts electronically, you must store them in a secure area on the NEP network.

11. Reporting suspected data security breaches

A data security breach may occur in relation to or as a result of e.g. theft of data (including physical copies), unsecured mode of transmission or an incorrect method of disposal of data or media.

If you become aware of a Personal Data (or other) data security breach or suspect that one has occurred, you must immediately report this to your Regional Privacy Champion, the IT Service Desk, ITSecurity@nepgroup.com and your line manager who might notify the competent data protection authority and the persons affected by the data security breach.

For further information about how to report suspected data security breaches see ***NEP's Security Incident Procedure***.

12. Ensure that Personal Data is accurate and kept up to date

Any inaccuracies in Personal Data held by NEP should be corrected by staff across all the relevant systems. Any updates or changes to information provided by an individual at any time should also be made on NEP's records.

Data subjects must be informed of their right to access, correct, erase or restrict the processing of their collected Personal Data.

13. Securely disposing of personal data

If Personal Data is no longer required, you must ensure that it is disposed of carefully and securely.

If any member of staff receives a request for information referencing any Data Protection Law please contact your Regional Privacy Champion immediately to ensure that it is properly dealt with within the prescribed time limits.

14. Privacy impact assessments

If you are establishing new processes, policies or procedures, embarking on a new project or purchasing new systems which involve handling or transferring large volumes of Personal Data or that could have a material impact on personal privacy or the security of Personal Data processed by or on behalf of NEP, then you should carry out a Privacy Impact Assessment ("**PIA**"). Please contact the Regional Privacy Champions. This could also occur if you are outsourcing a particular function or service or in the context of a significant procurement.

Docusign Envelope ID: 4B6B92CF-BAE9-815D-81D2-4C6F9CB5EB49

15. Training

You must attend all courses regarding the protection and handling of Personal Data which NEP asks you to attend. These may include off site and e-learning courses.

16. Data protection and disciplinary action

If any individual contravenes (or is suspected of having contravened) any aspect of this Policy, appropriate disciplinary action may be taken in accordance with the relevant disciplinary procedure.

Depending on the seriousness of the conduct, disciplinary action may result in dismissal without notice.

NEP also reserves the right to take such other action against an individual short of dismissal (including removing the right of authorised access to Personal Data) as may be appropriate in the circumstances.

If any individual has any doubts about whether he or she is processing Personal Data fairly and lawfully, they should contact your Regional Privacy Champion before carrying out any processing.

17. Changes to this data protection policy

This Policy is reviewed by Group Legal on a regular basis. You will be notified of any significant changes to the Policy via NEP's website.

Approval for implementation of this Policy has been given by:

Signed by:

Chief Executive Officer — November 19, 2026 — Date

DocuSigned by:

Chief Legal Officer — November 20, 2026 — Date