Policy Title:	**Data Protection Policy**
Policy Owner:	**General Counsel and SVP, Human Resources**
Department:	**Legal and Human Resources**
Implemented:	**May 24, 2018**
Revision Date:	
Next Review Date:	**May 24, 2019**

DATA PROTECTION POLICY: GENERAL RULE

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

For more details and further information, please read the body of this policy.

TABLE OF CONTENTS:

EXPLANATORY NOTE AND STATUS OF THIS POLICY

NEP Group, Inc. together with its subsidiaries 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.

Subject to applicable law, this Policy applies to all NEP employees (full-time and part-time), temporary workers, contractors, volunteers, interns, visitors, vendors and other third parties.

For NEP locations where applicable law requires specific policies and/or procedures in lieu of or in addition to this Policy, country-specific addendums may be attached to this Policy.

PART A –NEP'S RESPONSIBILITY TO YOU UNDER DATA PROTECTION LAWS

1. Data Privacy Team

NEP has appointed a team of Data Protection Champions to help it comply with its obligations under the Data Protection Laws. The key role of the Data Protection 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;
- to deal with information access requests; and

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 local Data Protection Champion.

Your Data Protection Champion can be found by contacting Legal, HR or IT.

2. Scope of the data protection laws

Data Protection Laws govern the way in which NEP may process information that identifies or is about living individuals (Personal Data) and also gives those individuals certain rights and remedies in respect of

that information. The laws also regulate marketing activities, and the use of on-line tracking technologies such as cookies. They therefore cover a very wide range of activities which NEP (and its partners and suppliers on NEP's behalf) undertake.

The laws impose a higher standard of care in relation to the use of "**Sensitive Personal Data**" which includes information concerning an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic and biometric data and, for the purposes of this policy, criminal convictions and offences. In this policy, references to "**Personal Data**" covers activities undertaken with all types of information about individuals including Sensitive Personal Data.

Data Protection Laws regulate information stored by or on behalf of NEP electronically or, in certain situations, stored as part of certain types of well-structured manual filing systems. CCTV footage and audio recordings are also covered.

3. The type of information NEP may hold about its staff

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, National Insurance number / national I.D number, immigration status, marital status, next of kin;
- personnel records including training, appraisal, photos, performance and disciplinary information, disability information, resumes and succession planning;
- bank details, salary, bonus, benefits and pension details;
- CCTV images and call recordings;
- Travel history, copies of passports, copies of driving licenses, password identifiers and VISA eligibility information.
- Sensitive Personal Data such as information on racial or ethnic origin, religious or philosophical beliefs, trade union membership, health, genetic and biometric data and criminal convictions or offences.

4. The manner in which NEP may process staff Personal Data

Personal Data about individuals may only be processed for a legitimate purpose. NEP will undertake a number of activities with a member of staff's Personal Data including, but not limited to:

- salary, benefits and pensions administration;
- health and safety records and management;
- criminal records checks, credit checks and clearances (where applicable);

- confirming information on resumes, curriculum vitaes and covering letters, providing reference letters and performing reference checks;
- training and appraisal, including performance evaluation and disciplinary records;
- staff management and promotions;
- succession planning;
- 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;
- other disclosures required in the context of staff employment promoting or marketing of NEP, its products or services;
- provision of staff information to customers and agencies in the course of the provision of NEP's services;
- CCTV monitoring for security reasons;
- operation of any ethics or whistleblowing hotline which NEP may run now or in the future;
- compliance with applicable procedures, laws, regulations, including any related investigations to ensure compliance or of any potential breaches;
- establishing, exercising or defending NEP's legal rights;
- any other reasonable purposes in connection with an individual's employment or engagement by NEP;
- providing and managing use of services provided by third parties, such as travel companies, company provided mobile phones, company credit cards and company cars and billing for such services.

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.

In order to fulfil these purposes, NEP reserves the right to disclose at its discretion an individual's Personal Data (or sensitive personal information as appropriate) to law enforcement agencies, regulatory bodies, government agencies and other third parties as required by law or for administration purposes, to the extent local law allows and requires.

NEP may also provide Personal Data in particular for, but not limited to, the same purposes as set out above, to contractors and suppliers that provide services to NEP and who may assist in the processing activities set out above. In such a case, NEP is additionally engaged to enter into a data processing agreement with the contractors and suppliers to whom NEP provides Personal Data.

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**") (defined for these purposes to include the UK) for the purposes of:

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

These countries may include, among others, the countries in which NEP has operations, and the location of our suppliers and their data centres, such as Microsoft (US), complete with other larger vendors of HR software.

Please note that the laws of some jurisdictions outside the EEA may not be as protective as Data Protection Laws in the EEA.

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.

6. Monitoring

Monitoring of NEP's systems

NEP's IT and communications systems are intended to promote effective communication and working practices within our organisation.

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, is monitored. If you access services by the use of passwords and login names on NEP's IT and communication systems this might mean that your personal access details are seen by NEP.

Monitoring is only carried out if and to the extent permitted or as required by law and as necessary and justifiable for business purposes. This is required so that instances of attempted misuse and other security events can be detected and that information is available to support any subsequent investigation and follow up actions. To the extent permitted by law and, where breaches of this Policy are found, action may be taken under the disciplinary procedure.

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 (this list is not exhaustive):

- 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.

If necessary such information may be handed to the police or other law enforcement agency. Investigations and disclosure of information to the relevant authorities shall be carried out only to the extent permitted by law.

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. 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 members of staff may be entitled to ask NEP for a copy of their Personal Data, to correct it, erase or restrict its processing, or to ask NEP to transfer some of this information to other organisations. Staff may also have rights to object to some processing of their Personal Data and, where NEP has asked for their consent to Process 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 the member of staff withdraws their 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.

For any concerns or questions about how NEP processes staff Personal Data, please contact the Data Protection Team.

8. Grievances

Any individual worker who believes that another person may have infringed their data protection rights is encouraged to bring this to the attention of their line manager or such other person as specified within the business unit/local grievance procedure.

Employees with unresolved concerns also 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

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 the Data Protection Laws. It is important that individuals are aware of their own data protection responsibilities towards others under the 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 the 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.

Your general responsibilities are as follows:

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 is was 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 EEA if that 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 11 (Reporting suspected data security breaches) relate not just to Personal Data but to all information, IT and communications systems that you are responsible for 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 from outside our premises.
- 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.

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 other passengers, and you should take appropriate precautions in the 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, by using a network provided by a reputable company and which is preferably locked down 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:
    - user names/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 Personal Data away 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:

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.

Restrictions on use of unauthorised devices or software:

- 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.

Third-party access:

- 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 your Data Protection Champion for guidance on the provisions required.
- 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 a 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 Personal 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 should be where possible disposed of using confidential waste bins or by using paper shredders.

- 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.
- 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
    - use must not commit NEP to any marginal costs.
- All email traffic related to business activities must be through an approved corporate email system.

Customer contact details:

- You must either 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 NEP network.

11. Reporting suspected data security breaches

A data security breach may occur in relation to or as a result of any of the following events (this list is not exhaustive):

- Theft of data (including physical copies) or equipment (laptops, mobile phones, memory sticks, CD-ROMs, etc.) on which data is stored;
- User ignorance/lack of training;
- Unauthorised access/copying;
- Incorrect security classification/marking/labelling;
- Unsecured mode of transmission;
- Use of uncontrolled or unauthorised media;
- Loss, or possible loss, of media, devices or equipment;
- Loss or possible loss of backup media;
- Inappropriate retention of information;
- Misdirection/misrouting of Personal Data;
- Incorrect method of disposal of data or media;
- Hacking/interception;
- Eavesdropping/espionage;
- Inappropriate release to the public domain;
- Access by unsupervised maintainers/contractors;
- Inappropriate access controls allowing unauthorised use by members of staff or others; or
- Information obtained by deceiving NEP.

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 Data Protection Champion and your line manager who might notify the competent data protection authority and the person affected by the data security breach. It is your responsibility to ensure that the report is received and that the Data Protection Champion and your line manager are actively aware that it has been sent (sending an email or leaving a voice message may be insufficient if you cannot be sure the recipient has picked up the message – always check).

You should try to provide as much information as possible (including but not limited to the following information):

- What type of data was involved (whether sensitive or otherwise);
- When did the security breach happen;
- How did the breach occur (e.g. if data has been stolen or lost or whether unauthorised access is suspected);
- If the data has been damaged or corrupted, in what way has it been damaged or corrupted;
- How many individuals' Personal Data are likely to be affected by the breach;
- Who are the individuals whose data has been lost (i.e. are they are they staff, customers, clients or suppliers);
- Steps taken or to be taken to prevent further issues, whether the breach is a repeat occurrence or if further data is being affected; and
- Any known contractual commitments given to third parties regarding the security of the Personal Data (e.g. to NEP's customers).

You should then assist in stopping or mitigating the data security breach.

12. Ensuing individuals know how their data will be used by NEP

In certain circumstances the express consent of individuals will be required. NEP has standard privacy statements and clauses which it has incorporated into its standard contracts to ensure this requirement is met and provide guidance to those who need to know when express consent should be obtained.

13. 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.

14. 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 Data Protection Champion immediately to ensure that it is properly dealt with within the prescribed time limits.

15. 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 refer to NEP's PIA guidance. This could also occur if you are outsourcing a particular function or service or in the context of a significant procurement.

16. 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.

17. External guidance from your local data protection authority

There are a number of useful guidance notes on the website of the European Data Protection Board, the UK's ICO and other data protection authorities.

18. 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 the Data Protection Team before carrying out any processing.

19. Monitoring and review of this Policy

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

APPROVAL

Approval for implementation of this Policy has been given by:

_____	_____
Chief Executive Officer	Date
_____	_____
General Counsel and Chief Compliance Officer	Date
_____	_____
Senior Vice President of Human Resources	Date

Revision History

Date	**Revision Summary** (begin with Section Number/Title)
May 1, 2018	Policy effective