Author:	Claire Johnson	Version:	3
Edit Date:	15/02/2021	Review Date:	15/02/2022
Director Approval:	Ashley Robertson		

National End-Point Assessment (NEPA) are committed to being transparent about how personal data is collected and used, ensuring they are meeting its data protection obligations. This policy sets out the company's commitment to data protection and the individuals rights and obligations in relation to how personal data is used throughout the end point assessment process.

This policy applies to all personnel whose data NEPA process regardless of whether it relates to current, past, or present employees, employers or apprentices.

Definitions

Data Protection Legislation

The General Data Protection Regulation ("GDPR") and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and (iii) any successor legislation to the GDPR or the Data Protection Act 2018.

Data Subject

A living identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data. This could be you, your colleagues, customers, and suppliers or indeed any other person.

Personal Data

Any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access, including but not limited to, data held in a filing system. Personal Data includes Special Categories of Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. This could include information in an electronic, paper or other format (e.g. images, multimedia, etc.)

Personal Data Breach

Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of Personal Data.

How Will NEPA Process Personal Data?

NEPA will process personal data in accordance with the following data protection principles:

- NEPA will process personal data lawfully, fairly and in a transparent manner.
- NEPA will collect personal data only for specified, explicit and legitimate purposes.
- NEPA will process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- NEPA will keep accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- NEPA will keep personal data only for the period necessary for processing.
- NEPA will adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

NEPA will inform individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its Privacy Notices. It will not process personal data of individuals for other reasons.

NEPA will update personal data promptly if an employee advises that his/her information has changed or is inaccurate. The employee is under an obligation to keep the company updated of any changes to their personal data.

Personal data gathered during employment or engagement as a worker, contractor, volunteer, apprentice or whilst on an internship, is held in the individual's personnel file (hard copy, electronic format or both) and on HR systems. The periods for which the company holds personal data are contained in its Privacy Notices as issued to individuals at the point data is collected, or at other points as the company deems its obligations require.

Process for Requesting a Data Subject Access Request

All individuals have the right to make a subject access request. If an individual makes a subject access request, NEPA will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual
- to whom his/her data is or may be disclosed, including recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers.
- for how long his/her personal data is stored (or how that period is decided)
- his/her rights to rectification or erasure of data, or to restrict or object to processing.
- his/her right to complain to the Information Commissioner if he/she thinks the company has failed to comply with his/her data protection rights.
- whether or not the company carries out automated decision-making and the logic involved in any such decision-making

NEPA will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless he/she agrees otherwise.

To make a subject access request, the individual should send the request to *arobertson@nationalepa.co.uk*

In some cases, NEPA may need to ask for proof of identification before the request can be processed. NEPA will inform the individual if it needs to verify his/her identity and the documents it requires.

NEPA will normally respond to a request within 30 days from the date it is received.

If an employee of NEPA receives a Data Subject Access request, they must immediately inform Ashley Robertson and take steps to comply with the above response procedure.

How Will NEPA and its Employees Process Personal Data?

Everyone who works for, or on behalf of, the company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the company's Data Security and Data Retention policies.

The Managing Director is responsible for the implementation of any actions relating to this policy and updating all staff about their data protection responsibilities and any risks in relation to the processing of data. NEPA employees should direct any questions in relation to this policy or data protection to this person. All NEPA staff should always ensure the following in line with this policy:

- NEPA employees should only access personal data if you need it for the work you do for, or on behalf of the NEPA and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
- NEPA employees should not share personal data informally.
- NEPA employees should keep personal data secure and not share it with unauthorised people.
- NEPA employees should regularly review and, where required or requested, update personal data you deal with. This includes telling us if your own contact details change.
- NEPA employees should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- NEPA employees should use strong passwords and not share your passwords with any other person.
- NEPA employees should lock your computer screens when not at your desk.
- NEPA employees should consider anonymising data or using separate keys/codes so that the Data Subject cannot be identified.
- Do not save personal data to your own personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of Ashley Robertson.
- NEPA employees should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- NEPA employees should not take personal data away from company's premises without authorisation from you're the Managing Director.
- Personal data should be shredded and disposed of securely when you have finished with it.

If any NEPA employees have concerns or are unsure about any aspect of data protection or security, they should ask for help from the Data Protection Officer/Data Protection Manager.

Any deliberate or negligent breach of this policy may result in disciplinary action being taken against the staff member in accordance with the disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in dismissal.

For What Reasons Can Personal Data be Collected or Processed?

- Personal data must be collected only for specified, legitimate purposes.
- Personal data cannot be used for new, different or incompatible purposes from that discloses when it was first obtained, unless you have informed the data subject of the new purposes and they have consented where necessary.

Is There a Limit to The Amount of Personal Data That Can be Collected and Processed?

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed (end- point assessment).

- Personal data must only be processed when performing job duties requires it. Processing personal data for any reason unrelated to your job duties is not permitted.
- Excessive data must not be collected. Ensure any personal data collected is adequate and relevant for the intended purposes.
- When personal data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the company's data retention guidelines.

Data Sharing

NEPA will only share data based on the following conditions:

- For the delivery of apprenticeship certification, we will share the following information with the Education and Skills Funding Agency and the Institute for Apprenticeship and Technical Education.
    - Apprentice name,
    - Unique learner number,
    - Date of birth,
    - Employer name
    - Any other information required including details of name changes and proof of changes.
- Prior to end-point assessment, if reasonable adjustments are required, we will request detail of the difficulty and/or disability in the context of the reasonable adjustment required. This data will be shared with your employer/provider and NEPA to ensure that the reasonable adjustments can be agreed and put in place. No information on difficulties/disabilities can be submitted to NEPA without the apprentice's consent.
- NEPA will share your name and employer with the assessors so that we can check for any potential conflicts of interest in assessment.
- NEPA will share anonymised data on assessment results with our external quality assurance provider and for our own monitoring and quality assurance purposes.

How Long Can Personal Data be Stored?

Under guidance for end-point assessment, personal data will be kept for 6 years. Personal data must not be kept longer than necessary for the purposes for which the data is processed.

What Should Happen in the Event of a Data Breach Occurring?

If NEPA suspects or discovers that there has been a breach of personal data, and that this could pose a risk to the rights and freedoms of individuals, we will report the breach to the Information Commissioner within 72 hours of discovery. NEPA will record all data breaches regardless of their effect and employees must therefore report any breach, regardless of any perceived level of severity.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, NEPA will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Any person employed by NEPA who knows or suspects that a personal data breach has occurred, should not attempt to investigate the matter themselves. They should immediately contact the person or team designated as the key point of contact for personal data breaches. All evidence relating to the potential personal data breach should be preserved. Failure to notify the designated person or team may result in disciplinary action being taken.

Will NEPA Take Disciplinary Action if There is a Data Breach?

No disciplinary action would automatically be taken simply as a result of a breach having occurred. An investigation would first need to be carried out, to establish the causes of the breach.

Where investigation reveals that a data breach has been caused (wilfully or negligently or without due care and attention) through an employee's actions or inactions, this may lead to disciplinary action being taken. In the event of a serious breach and/or a failure to follow the appropriate procedures NEPA has put in place for data processing, this could amount to an offence of gross misconduct.

Failure to report a breach, or suspected breach, could result in disciplinary action. In serious cases this could amount to an offence of gross misconduct.

NEPA use secure portals for the collection and storage of data. For further information on data storage contact *www.ACE360.co.uk*

This policy will be reviewed annually as a minimum.