National Extension College

Data Protection and Privacy Policy

VERSION : 3.1
LAST REVISED: JUNE 2026
NEXT REVIEW DATE: JUNE 2027

DATA PROTECTION AND PRIVACY POLICY

1. POLICY STATEMENT

The Data Protection & Privacy policy is to ensure that the company, its staff, students and tutors and their information is protected, and that NEC and its staff comply with Data Protection Act 2018 (which now incorporates UK GDPR) and the Data (Use and Access) Act 2025 (DUAA),in relation to how it collects, stores and deals with data.

2. SCOPE

This policy covers all information that can be identifiable to a particular individual whatever form the information is recorded, whether that is in IT systems, paper documents, forms or written in notebooks. It also covers people's information rights and the basis for processing data.

Staff must only collect personal data when necessary for business operations (minimising data held). Personal data must be stored securely, retained only for as long as necessary, and never shared carelessly. Any staff member processing data must comply with the Data Protection principles

Managers must consider data protection for all relevant policies, and when designing and implementing new systems, products and practices that involve personal data.

3. DEFINITIONS OF DATA PROTECTION TERMS

Data subject - someone who can be identified from personal data. The data could be their name, address, telephone number or something else – but if it's about a person (customer, employee, service users), then they're the data subject.

Processing - taking any action with someone's personal data. This begins when a data controller starts making a record of information about someone, and continues until you no longer need the information and it's been securely destroyed.

Data controller - has the responsibility of deciding how personal data is processed and protecting it from harm. Controllers can delegate the processing of personal data to data processors, but the responsibility for keeping it safe will still rest with the controller. In most cases this will be NEC.

Data processor - In a similar way to data controllers, data processors have to protect people's personal data – but they only process it in the first place on behalf of the controller. For example, data processors could be IT support companies, payroll providers or another service where personal data is used.

4. INFORMATION SENSITIVITY

Under General Data Protection Regulations (GDPR) information falls into these categories:

- *Personally Identifiable.* Information that identifies the data subject and personal information such as name, address, gender, date of birth.
- *Special Categories*. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- *Prisoners and Convictions*. This is determined by 'Member State law' (Article 10). The UK Data Protection Bill essentially puts it in special categories.
- *Under-16s.* Any information about under-16s must have explicit consent from a parent or guardian. For consistency with other regulations NEC will obtain consent for under-18s

5. RESPONSIBILITIES

NEC and its data processors have a number of responsibilities:

Transparency - NEC publishes very detailed collection points in its Privacy Notice on its website to be clear on how we process, store and use data - which can be found at https://www.nec.ac.uk/policies

Legal basis and consent - NEC must have a legal basis to hold the data. We only hold data to provide a service, specifically a course (based on signing up to a course, and thus a contract) or an Exam, UCAS or Tutorial related service. We will also hold data to allow students to rejoin (for continuation of the next stage of their studies to the next level). All data is deleted or anonymised after 2 years of course expiry. All data subjects need to consent to NEC holding information for both contract performance and/or for marketing purposes.

All staff have a responsibility to keep data safe and secure at all times.

NEC reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with these policies and procedures.

NEC reserves the right to monitor how its network, computer systems and applications are used in the event of a data breach.

6. INFORMATION LOCATION REGISTER

In order to comply with data protection procedures for subject access requests, accuracy and deletion, NEC will maintain an information location register of where all personally identifiable information is held, whether that is in systems, spreadsheets or on paper.

NEC keeps an Information Location Register which is central to all the data protection procedures and so it is essential that this is maintained. The information register will identify:

- The location of the information and who has access.
- The information sensitivity and legal basis.
- The business purpose for holding the information
- The retention period.
- Who has responsibility for maintaining the information, for access requests and to ensure deletion.

7. INFORMATION STORAGE & SHARING

The primary method of storing and sharing information is via the NEC Google Drive account which can be controlled and audited by NEC. Data transfer via file sharing must only be performed following permission of IT and the CEO.

Personal information must not be shared or transferred using memory sticks or other removable media

Where files are encrypted the decryption key must only be sent via a separate email, not in the same email as the file itself.

Chromebook data is encrypted by default, however, staff should still limit the level of information in the downloads or Google Drive data selected for offline access and only retain it whilst it is necessary (the care over Google Drive use applies to Staff, Tutors and Consultants). Staff, Tutors and Consultants must regularly delete downloads on their device and ensure their personal Google DRIVE is only used temporarily prior to transfer to a SHARED DRIVE (if a Staff Member) or deletion.
Paper reports and forms which hold personal information must be kept secured at all times.

8. DATA SUBJECT RIGHTS PROCEDURES

Requests or formal data complaints from data subjects must be made via our online portal here or via email to NEC using student.support@nec.ac.uk (or in writing to the NEC office). The request must be made by the data subject or, in the case of an under-18 student, the parent or guardian.

The request will be managed by Student Support (for students, sponsors and tutors) or HR (for staff and consultants) who will coordinate the information retrieval and act as required using the Information Location Register.

8.1 Statutory Data Protection Rights

UK GDPR gives individuals specific rights over their personal data. For general data processing, in summary these are:

- The right to access personal data held about them (the right of subject access);
- The right to be informed about how and why their data is used - and you must give them privacy information;
- The right to have their data rectified, erased or restricted;
- The right to object;
- The right to portability of their data; and
- The right not to be subject to a decision based solely on automated processing.

All standard rights requests (such as Subject Access Requests or Rectification requests) will be actioned and completed within 28 days (or sooner) following the receipt of the request from the data subject. If the data subject is currently enrolled on a course, deletion will require the course to be cancelled and in this case NEC will need to seek confirmation of that intention. When the request is confirmed all information on all systems and locations will be deleted within 28 days, with the exception of system backups which will be overridden upon the next backup.

8.2 Statutory Right to Complain (DUAA 2025 Requirements)

Under the Data (Use and Access) Act 2025, individuals have a formalised statutory right to lodge a complaint with NEC regarding how their personal data is handled (including dissatisfaction with marketing opt-outs or how a rights request was processed).

To comply with these legal requirements, NEC operates under the following statutory framework:

- Mandatory First Step: Data subjects must submit their complaint directly to NEC first via our dedicated Google Form or email path to allow for an internal investigation before the matter can be escalated to the regulator.
- 30-Day Acknowledgement Window: NEC is legally required to formally acknowledge all data protection complaints within 30 calendar days of receipt.
- Investigation and Resolution: NEC will investigate the concerns raised without undue delay. The data protection lead will communicate a meaningful outcome and detail any remedial actions taken directly to the complainant.
- ICO Escalation: NEC will include Information Commissioner's Office (ICO) escalation details in its final complaint responses. If the data subject remains dissatisfied with NEC's final internal conclusion, they maintain the right to escalate their complaint directly to the ICO (www.ico.org.uk).

NEC uses its Privacy Notice on its website to explain transparently how it handles individual data and processes these complaints.

9. OBTAINING AND RESTRICTING CONSENT

Certain information requires the consent of the data subject. Consent must be obtained and recorded for each purpose. Consent may be withdrawn by the data subject, parent or guardian. Withdrawing consent may have service implications on live courses.

10. INFORMATION RETENTION AND DESTRUCTION

Other than specific retention for consent, performance of contract and special categories of information covered under consent. NEC will retain student contact and enrolment information to meet mandatory and regulatory data requirements. It will review information retention based on likelihood of re-enrolment and continued use of services. This enables NEC to:

- Provide reference information on previous students enrolment on NEC courses.
- Provide reprints of course completion certificates.
- Enable students returning to have the same login details and to access the materials of their previous courses.

Once the retention period is over all contact information will be deleted from all systems, spreadsheets and documents on systems and paper.

11. INFORMATION BREACH REPORTING

An information breach is any instance where personally identifiable information has been lost or compromised (including loss of an NEC device). It also applies where the risk of compromise has been increased.

A central record will be kept of all personal data breaches, even trivial ones, to allow trend monitoring. In alignment with our DUAA obligations, this log will run alongside NEC's central Data Complaints Log to ensure comprehensive compliance reporting for the ICO.

Any data breach (including lost assets containing data) must be reported within 72 hours to the ICO. The NEC's SMT will assess whether a breach is reportable to ICO (depending on what has occurred). SMT will also inform all relevant parties. Staff and Consultants must complete the breach form and notify their manager and the CEO immediately upon the discovery of the breach. Tutors must report breaches immediately via tutor.support@nec.ac.uk email address.

12. Artificial Intelligence (AI) and Automated Processing

12.1 Transparency and Usage NEC may utilize Artificial Intelligence (AI) and machine learning technologies to enhance the educational experience and operational efficiency. This includes, but is not limited to:

- Learning Analytics: Processing engagement data to identify students who may require additional support.
- Student Support: Utilizing automated chatbots to assist with common inquiries.
- Grading Assistance: Employing AI tools to support tutors in providing timely feedback, though final academic grading remains a human-led process.

12.2 Automated Decision-Making and Opt-out Rights Under UK GDPR, you have the right not to be subject to a decision based solely on automated processing which produces legal or similarly significant effects.

- NEC does not currently use AI to make "solely automated" academic or enrollment decisions without human intervention.
- If such systems are introduced, data subjects will be notified and provided with a specific right to request human review or to opt-out where applicable

13. MONITORING AND REVIEW OF THE POLICY

We will continue to review the effectiveness of this policy to ensure it is achieving its objectives.