Data Security Policy

Policy last updated: August 2023
Review date: August 2024

Person responsible for Data protection: Gareth Lindsay (Managing Director)

NLTG Data Protection Officer (DPO): Tim Cutler (Quality Manager)

NLTG needs to collect and use certain types of personal information about the Individuals or Service Users who come into contact with NLTG in order to carry out their work/duties. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this complies with GDPR Data Protection Policy.

All data is collected in line with NLTG's GDPR Data Protection Policy (This includes checking information and data is securely hosted in the UK).

Questions about this policy, or requests for further information, should be emailed to dataenquiries@nltg.co.uk.

Data Storage

ESFA's use and access to learners personal data and details of organisations with whom they regularly share data , information about how long the ESFA retain learner data, and how learners can change their consent to being contacted is via https://www.gov.uk/government/publications/esfa-privacy-notice

Details of how NLTG process and store learners personal data is detailed in our Learner Privacy Notice accessible via www.nltg.co.uk/publications .

The above information is detailed within learner enrolment/application forms that applicants complete as part of learner recruitment arrangements.

Staff personal information and records will be stored securely and will only be accessible to authorised staff and volunteers i.e. work experience (whom have signed a confidentiality agreement).

Information will be stored for only as long as it is needed, as detailed in the privacy policies, and will be disposed of appropriately.

Staff and learners information may be stored on:

- **Mobile devices such as laptops, tablets and mobile phones**
  NLTG have stringent policies in place to ensure that all devices are password protected, updated regularly and are running sufficient malware protection.
  The devices are also monitored daily by system administration and protection software.
  To be read in conjunction with Computer Policy, Mobile Phone Policy, Internet & Email policy
- **Network Servers**
  All servers are password protected and can only be accessed remotely by a member of the IT Admins Security group.
  All servers are updated, patched regularly and backed up daily.
  All server rooms are physically locked and only accessible by authorised personnel.
- **Cloud Networks (Microsoft SharePoint) ***
  All data transferred to Microsoft SharePoint uses their encryption to ensure the data remains safe and secure.

- **Online Portfolio ***
  Learning Assistant (LA) is an online portfolio system owned by City & Guilds.
- **Aptem***
  End to end platform system including e-portfolio

- **Physical Paperwork**
  All physical copies of paperwork are either scanned and stored on SharePoint or stored in locked filing cabinets/rooms that are only accessible by authorised members of staff.
- **External Systems (i.e. People's Inc, Scottish Widows, Hunter Southall) ***
  All these systems are vetted to ensure safe transport of data is maintained and each use encrypted software to transfer and store information securely.

  **Governed by the suppliers GDPR data protection policies and procedures.*

Transferring of Personal Information

The need may arise where personal information has to be shared with authorised and relevant bodies, as per GDPR Policy https://www.nltg.co.uk/publications/data-protection-gdpr-policy/.

Where applicable, this will be done via the external organisation's secure portal. If information has to be sent via email, then this will be encrypted, and password protected.

Destruction of Data

It is NLTG's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the group. If computer equipment is being passed on/sold to a third party, a full system wipe will be carried out by IT Services which will be verified by a second person. If a computer system is being destroyed or paperwork needs to be destroyed, this will be carried out by a registered company and proof of destruction will be obtained.

Extrinsic Assurance

NLTG are compliant with the requirements of the Cyber Essentials Scheme and have undergone intensive external assessment to ensure that our systems are up to standards to obtain certification.
Certification registration number available upon request.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under NLTG's disciplinary procedure. Significant or deliberate breaches of this policy may constitute gross misconduct as listed within the companies' disciplinary procedure and could lead to dismissal without notice.

Should a breach occur please notify IT Services and the Data Protection Officer. If a breach is identified out of working hours, please call the out of hours number 07548 562632.

Associated Documentation

NLTG GDPR Policy (NL0500 a)
Learner Privacy Notice
Employee Privacy Notice
Computer Policy (NL0500 i (ii))
Mobile Phone Policy (NL0500 i (vi))
iPad Policy (NL0500 i (v))
Email and Internet Policy (NL0500 i (i))
Microsoft Trust Centre
City & Guilds

Signed _____
GARETH LINDSAY
NLTG Managing Director