Data Protection Policy Statement

This policy is available on our website:

https://www.ngtc.co.uk/student-services/our-policies/

or scan the QR code

Author ID: LJ

Version: 3.4

Last Review Date: December 2025

Next Review Date: December 2026

Summary of Changes

Date	Page(s)	By	Details of Amendments
01/12/2023	n/a	MN	Annual Review
15/12/2024	n/a	LJ	Annual Review
15/12/2025	n/a	LJ	Annual Review
	All	BT	Minor formatting and grammatical amendments

1. Introduction

1.1 Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2 Definitions used by the organisation (drawn from the GDPR)

Material scape (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services or monitor the behaviour of data subjects who are resident in the EU.

1.3 Article 4 definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural personal is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, 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.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration,unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent – means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing or personal data.

Child - the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is

only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third Party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority or the controller or processor, are authorised to process personal data.

Filing System – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. Policy Statement

2.1 The Board of Directors and management of NGTC as a whole, located at Dorbcrest House, 20 Lowe Mill Lane, Hindley, Wigan, WN2 3AF are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information NGTC collects and processes in accordance with the General Data Protection Regulation (GDPR).

2.2 Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy, along with connected processes and procedures.

2.3 The GDPR and this policy apply to all of NGTC's personal data processing functions, including those performed on customers', clients', employees' suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

2.4 NGTC has established objectives for data protection and privacy, which are in PIMS and GDPR Objectives record.

2.5 Data Protection office is responsible for reviewing the registers of processing annually in the light of any changes to NGTC's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments.

2.6 This policy applies to all Employees of NGTC. Any breach of the GDPR will be dealt with under NGTC's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.7 Partners and any third parties working with or for NGTC, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data help by NGTC without having first entered into a data confidentiality/individual user agreement, which imposes on the third-party obligations no less onerous than those to which NGTC is committed, and which gives NGTC the right to audit compliance with the agreement.

3. Responsibilities and roles under the General Data Protection Regulation

3.1 NGTC is a data controller and data processor under the GDPR.

3.2 Top Management and all those in managerial or supervisory roles throughout NGTC are responsible for developing and encouraging good information handling practices within NGTC; responsibilities are set out in individual job descriptions.

3.3 Data Protection Officer, a role specified in the GDPR, should be a member of the senior management team, is accountable to Board of Directors of NGTC for the management of personal data within NGTC and for ensuring that compliance with data protection legislation and good practice can be demonstrated.

This accountability includes:

- 3.3.1 development and implementation of the GDPR as required by this policy; and
- 3.3.2 security and risk management in relation to compliance with the policy.

3.4 Data Protection Officer has been appointed to take responsibility for NGTC's compliance with the policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that NGTC complies with the GDPR, as do Manager's in respect of data processing that takes place within their area of responsibility.

3.5 The Data Protection Officer have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees seeking clarification on any aspect of data protection compliance.

3.6 Compliance with data protection legislation is the responsibility of all Employees of NGTC who process personal data.

3.7 Employees of NGTC are responsible for ensuring that any personal data about them and supplied by them to NGTC is accurate and up to date.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. NGTC's policies and procedures are designed to ensure compliance with the principles.

4.1 Personal data must be processed lawfully, fairly and transparently.

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the ''conditions for processing'', for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applied whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

NGTC Privacy Notice Procedure is set out in Policy Procedure and the Privacy Notice is recorded in Privacy Notice.

The specific information that must be provided to the data subject must, as a minimum, include:

- 4.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;
- 4.1.2 the contact details of the Data Protection Officer;
- 4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- 4.1.4 the period for which the personal data will be stored;
- 4.1.5 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- 4.1.6 the categories of personal data concerned;
- 4.1.7 the recipients r categories of recipients of the personal data, where applicable;

- 4.1.8 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- 4.1.9 any further information necessary to guarantee fair processing.

4.2 Personal data can only be collected for specific, explicit and legitimate purposes. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of NGTC's GDPR register of processing. Privacy Procedure sets out the relevant procedures.

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing

4.3.1 The Data Protection Officer is responsible for ensuring that NGTC does not collect information that is not strictly necessary for the purpose for which it is obtained.

4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.

4.3.3 The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay.

4.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

4.4.2 The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

4.4.3 It is also the responsibility of the data subject to ensure that data held by NGTC is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

4.4.4 Employees/learners/customers should be required to notify NGTC of any changes in circumstances to enable personal records to be updated accordingly. It is the responsibility of NGTC to ensure that any notification regarding change of circumstance is recorded and acted upon.

4.4.5 The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

4.4.6 On at least an annual basis, the Data Protection Office will review the retention dates of all the personal data processed by NGTC, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely delivered/destroyed in line with the Secure Disposal of Storage Media Procedure.

4.4.7 The Data Protection Office is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not the be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

4.5.1 Where personal data is retained beyond the processing data, it will be either minimised, encrypted or pseudonymised in order to protect the identity of the data subject in the event of a data breach.

4.5.2 Personal data will be retained in line with the Retention of Records Procedure and, once its retention data is passed, it must be securely destroyed as set out in this procedure.

4.5.3 The Data Protection Office must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

4.6 Personal data must be processed in a manner that ensures the appropriate security.
The Data Protection Officer will carry out a risk a risk assessment considering all the circumstances of NGTC's controlling or processing operations.

In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on NGTC itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the Data Protection Officer will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to NGTC.

When assessing appropriate organisational measures, the Data Protection Officer will consider the following:

- The appropriate training levels throughout NGTC;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace.
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability).

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility. NGTC will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

5. Data Subjects' Rights

5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- 5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- 5.1.2 To prevent processing likely to cause damage or distress.
- 5.1.3 To prevent processing for purposes of direct marketing.
- 5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- 5.1.5 To not have significant decisions that will affect them taken solely by automated process.
- 5.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.
- 5.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- 5.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened
- 5.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- 5.1.10 To object to any automated profiling that is occurring without consent.

5.2 NGTC ensures that data subjects may exercise these rights:

5.2.1 Data subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how NGTC will ensure that its response to the data access request complies with the requirements of the GDPR.

5.2.2 Data subjects have the right to complain to NGTC related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the GDPR Complaints Procedure.

6. Consent

6.1 NGTC understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

6.2 NGTC understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or based on misleading information will not be a valid basis for processing.

6.3 There must be some active communication between the parties to demonstrate active consent. The privacy notice will be read and signed by each data subject who consents to the data processing. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

6.4 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exits.

6.5 In most instances, consent to process personal and sensitive data is obtained routinely by NGTC using standard consent documents e.g. when a new client signs a contact, or during induction for participants on programmes.

6.6 Where NGTC provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit, which may be no lower than 13).

7. Security of data

7.1 All employees are responsible for ensuring that any personal data that NGTC holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by NGTC to receive that information and has entered into a confidentiality agreement.

7.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:

- In a lockable room with controlled access; and/or
- In a locked drawer or filing cabinet; and/or
- If computerised, password protected in line with corporate requirements; and/or
- Stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media

7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees of NGTC. All Employees are required to lock PC screens when away from their desks/work space.

7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation.

7.5 Personal data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by GDPR before disposal.

7.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

8. Disclosure of data

8.1 NGTC must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind

whether disclosure of the information is relevant to, and necessary for, the conduct of NGTC's business.

8.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Office.

9. Retention and disposal of data

9.1 NGTC shall not keep personal data in a form that permits identification of data subjects for a longer period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 NGTC may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

9.3 The retention period for each category of personal data will be set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations NGTC has to retain the data.

9.4 NGTC's data retention and data disposal procedures will apply in all cases.

9.5 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

10. Data transfers

10.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one of more or the specified safeguards, or exceptions, apply:

10.1.1 <u>An adequacy decision</u>

The European Commissions can and does assess third countries, a territory and/or specific sectors within Third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons.

In these instances, no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

10.1.2 Privacy Shield

If NGTC wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

Assessment of adequacy by the data controller

In assessing adequacy, the UK based exporting controller should take account of the following factors:

- The nature of the information being transferred;
- The country or territory of the origin, and destination, of the information;
- How the information will be used and for how long;
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligation; and
- The security measures that are to be taken as regards the data in the overseas location.

10.1.3 Binding corporate rules

NGTC may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that NGTC is seeking to rely upon.

10.1.4 Model contract clauses

NGTC may adopt approved model contract clauses for the transfer of data outside of the EEA. If NGTC adopts the model contract clauses approved by the relevant supervisory authority there is an automatic recognition of adequacy.

10.1.5 Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- The transfer is necessary for the performance of a contract between the data subject and the controller of the implementation of pre-contractual measures taken at the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- The transfer is necessary for important reasons of public interest;
- The transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- The transfer is necessary in order to protect the vital interests of the data subject or of other personals, where the data subject is physically or legally incapable of giving consent.

11. Information asset register/data inventory

11.1 NGTC has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. NGTC'S data inventory and data flow determines:

- Business processes that use personal data;

- Source of personal data;
- Volume of data subjects;
- Description of each item of personal data;
- Volume of data subjects;
- Description of each item of personal data;
- Processing activity;
- Maintains the inventory of data categories of personal data processed;
- Documents the purpose(s) for which each category of personal data is used;
- The role of NGTC throughout the data flow;
- Any data transfers; and
- All retention and disposal requirements

11.2 NGTC is aware of any risks associated with the processing of particular types of people data.

11.2.1 NGTC assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data by NGTC, and in relation to processing undertaken by other organisations on behalf of NGTC.

11.2.2 NGTC shall manage any risks identified by the risk assessment in order to reduce the likelihood of a nonconformance with this policy.

11.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural personas, NGTC shall, prior to processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

11.2.4 Where, as a result of a DPIA it is clear that NGTC is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether NGTC may proceed must be escalated for review to the Data Protection Officer.

11.2.5 The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress or the quantity of data concerned, escalate the matter to the supervisory authority.

11.2.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level and the requirements of the GDPR.

12. Network and Device Cryptography in Compliance with GDPR

12.1 Encryption and Data Security Measures

NGTC recognises the paramount importance of safeguarding personal data under the guidelines set forth by the General Data Protection Regulation (GDPR). To ensure the security and confidentiality of personal data, NGTC employs robust encryption and data security measures in all network and device interactions.

12.2 Encryption of Data in Transit

All data transmitted across NGTC's networks, whether internal or external, is encrypted using industry-standard protocols. This cryptographic protection ensures that sensitive personal data remains confidential during transmission, mitigating the risk of interception or unauthorised access. NGTC employs secure communication channels, implementing Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols as appropriate.

12.3 Encryption of Data at Rest

Personal data stored on NGTC's servers, devices, and storage media is subject to encryption to maintain its confidentiality and integrity. This includes data stored on physical servers and databases. The encryption algorithms used adhere to best practices and corporate requirements, rendering the data unreadable in case of unauthorised access.

12.4 Key Management and Access Control

NGTC maintains stringent control over cryptographic keys used for encryption and decryption. Access to these keys is restricted to authorised personnel only, following the Access Control Policy. Key management practices are designed to prevent unauthorised access, misuse, or loss of keys, ensuring the ongoing protection of encrypted data.

12.5 Secure Device Management

All devices used to process and store personal data are required to adhere to NGTC's cryptographic policies. Devices, including computers, laptops and mobile devices, must

utilise strong encryption mechanisms to prevent unauthorised access in case of loss, theft, or disposal.

12.6 Off-Site Processing and Data Protection

Processing personal data off-site presents potential security risks. Staff members are explicitly authorised to perform off-site processing, and this authorisation is contingent upon adherence to encryption and data security measures in line with NGTC's policies. The use of encrypted communication channels and secure connections is mandatory when accessing personal data from remote locations.

12.7 Data Transfers and Cryptographic Protections

NGTC recognises that international data transfers require rigorous protection to meet GDPR standards. In the unlikely event of exporting data from the European Economic Area (EEA) to non-EEA countries, NGTC ensures that adequate safeguards are in place. This may include employing binding corporate rules, model contract clauses, or assessing the adequacy of third-party protection mechanisms. All data transfers are documented, detailing the security measures applied to protect personal data during transmission.

12.8 Data Protection Impact Assessments (DPIAs)

In compliance with GDPR, NGTC conducts DPIAs for processing activities involving personal data. These assessments evaluate potential risks to individuals' rights and freedoms and consider cryptographic measures to mitigate such risks. If processing activities involving sensitive personal data are likely to result in high risks, DPIAs are conducted before commencing such operations. Any concerns regarding potential damage or distress to data subjects are escalated to the Data Protection Officer for review.

12.9 Compliance and Continuous Improvement

NGTC is committed to upholding the principles of GDPR through the implementation of robust network and device cryptography practices. Regular audits, assessments, and reviews are conducted to ensure ongoing compliance and the alignment of cryptographic measures with the evolving landscape of data protection.

12.10 Data Subject Rights and Cryptographic Security

NGTC acknowledges that effective cryptographic measures play a vital role in upholding data subjects' rights and freedoms. By safeguarding personal data through encryption and security practices, NGTC ensures that data subjects' information remains confidential, protected, and in line with GDPR requirements.

13. Network Monitoring and GDPR Compliance

13.1 Proactive Network Surveillance

NGTC recognises the significance of vigilant network monitoring in maintaining compliance with the General Data Protection Regulation (GDPR). Continuous network surveillance is paramount for identifying and mitigating potential security breaches, unauthorised access, or data vulnerabilities.

13.2 Real-time Threat Detection

To safeguard personal data, NGTC employs cutting-edge network monitoring tools that provide real-time alerts for suspicious activities. These tools track network traffic patterns, user behaviour, and system activities, enabling rapid response to any anomalies that may pose a risk to data security.

13.3 Intrusion Detection and Prevention

NGTC's network monitoring systems incorporate intrusion detection and prevention mechanisms to detect unauthorised access attempts or malicious activities. These systems work in tandem with firewalls and other security measures to promptly neutralise threats and prevent unauthorised access to personal data.

13.4 Data Breach Detection and Notification

In line with GDPR requirements, NGTC's network monitoring practices extend to identifying potential data breaches. Rapid detection of breaches triggers an immediate response, including containment and notification protocols as outlined in NGTC's Data Breach Notification Procedure.

14. Network Firewalls and GDPR Compliance

14.1 Firewall Protection

NGTC maintains robust network firewalls as a foundational element of data security and GDPR compliance. Firewalls act as a protective barrier, controlling incoming and outgoing network traffic based on predefined security rules and policies.

14.2 Data Segmentation and Access Control

Firewalls are strategically configured to enforce data segmentation and access controls. Personal data is isolated from unauthorised access through firewall rules that restrict traffic to authorised users and services, minimising the risk of data exposure.

14.3 Application Layer Filtering

NGTC's firewalls incorporate application layer filtering to scrutinise data packets at a granular level. This deep inspection ensures that only valid and authorised application traffic is allowed, preventing potential exploitation of application vulnerabilities.

14.4 Intrusion Prevention

NGTC's firewalls include intrusion prevention systems that actively monitor network traffic for malicious or suspicious behaviour. These systems detect and block intrusion attempts, enhancing data protection and maintaining GDPR compliance.

14.5 Regular Firewall Audits

To ensure ongoing compliance, NGTC conducts regular audits of its firewall configurations and rules. These audits assess the effectiveness of firewall settings, identify potential vulnerabilities, and verify that the implemented controls align with GDPR requirements.

15. Malware Prevention and GDPR Compliance

15.1 Comprehensive Malware Defence

NGTC employs a multi-layered approach to malware prevention to safeguard personal data and comply with GDPR mandates. This approach encompasses a combination of endpoint protection, network defences, and user awareness.

15.2 Endpoint Protection Solutions

All devices connected to NGTC's network are equipped with advanced endpoint protection solutions. These solutions include anti-malware software, behaviour-based detection, and real-time scanning to prevent malware infiltration and execution.

15.3 Network-based Malware Detection

NGTC's network infrastructure includes malware detection mechanisms that monitor incoming and outgoing traffic for signs of malicious software. Suspicious files and attachments are quarantined or blocked, mitigating the risk of malware propagation.

15.4 User Education and Training

NGTC places significant emphasis on user education and awareness. Regular training programs educate employees about the risks of malware, phishing attacks, and social engineering, empowering them to recognise and report potential threats promptly.

15.5 Incident Response and Remediation

In the event of a malware incident, NGTC follows predefined incident response procedures. Malware is isolated, removed, and the affected systems are thoroughly inspected to prevent recurrence. If the incident involves personal data, NGTC adheres to its Data Breach Notification Procedure as per GDPR guidelines.

16. Allocation of User Access Privileges and GDPR Compliance

16.1 User Access Management

NGTC places paramount importance on allocating user access privileges in strict accordance with the General Data Protection Regulation (GDPR). Effective access control ensures that personal data is only accessible to authorised personnel, reducing the risk of unauthorised data exposure.

16.2 Principle of Least Privilege

NGTC adheres to the principle of least privilege, granting users the minimum access rights necessary to perform their designated tasks. This approach prevents over-privileged access and limits the potential impact of security breaches or unauthorised data handling.

16.3 Access Control Policies

NGTC enforces comprehensive access control policies to regulate user access to personal data. These policies define roles, responsibilities, and the specific data categories each role can access, ensuring that data access is aligned with job functions and GDPR requirements.

16.4 User Authentication and Authorisation

User authentication is a critical component of access control. NGTC employs strong authentication mechanisms such as multi-factor authentication (MFA) to verify users' identities before granting access to personal data. Authorisation controls are applied to ensure that authenticated users can only access data within their authorised scope.

16.5 Regular Access Reviews

To maintain GDPR compliance, NGTC conducts periodic access reviews. These reviews evaluate user access privileges, ensuring that they remain aligned with job roles and responsibilities. Any changes to access rights are documented and authorised by relevant personnel.

16.6 User Termination Procedures

NGTC's access management process includes well-defined procedures for user termination. When an employee or contractor leaves the organisation, their access privileges are promptly revoked to prevent unauthorised data access. This proactive approach safeguards personal data from potential insider threats.

16.7 Access Logs and Auditing

NGTC maintains comprehensive access logs and conducts regular audits to monitor user activity. These logs record data access, modifications, and system interactions, enabling traceability and accountability. Audits help identify unusual behaviour, potential security breaches, and ensure compliance with GDPR's accountability principle.

16.8 Data Classification and Access

NGTC classifies personal data based on its sensitivity and criticality. Access privileges are aligned with data classification levels, ensuring that only authorised personnel can access sensitive or confidential data. This practice maintains the confidentiality and integrity of personal data as mandated by GDPR.

16.9 Continuous Monitoring and Improvement

NGTC's commitment to GDPR compliance extends to ongoing monitoring and improvement of user access management. Feedback, incident reports, and security assessments inform adjustments to access control policies, reinforcing data protection measures.

16.10 Data Subject Rights and Access Control

NGTC's stringent access control measures play a pivotal role in upholding data subject rights. By strictly controlling who can access personal data, NGTC ensures that individuals' privacy rights are respected, and their personal information is safeguarded against unauthorised disclosure or misuse.

17. Storage and Destruction in Compliance with GDPR

17.1 Secure Data Storage

NGTC places paramount emphasis on secure data storage to comply with the General Data Protection Regulation (GDPR). Effective storage practices are pivotal in maintaining the confidentiality, integrity, and availability of personal data.

17.2 Controlled Storage Environments

NGTC ensures that personal data is stored in controlled environments. This includes lockable rooms, locked drawers or filing cabinets, and secure digital storage solutions. These measures prevent unauthorised physical and digital access, aligning with GDPR's security principles.

17.3 Encryption of Stored Data

Personal data stored in digital formats is subject to encryption. NGTC employs encryption algorithms that adhere to industry standards to render stored data unreadable in case of unauthorised access. This cryptographic protection mitigates the risk of data breaches and unauthorised disclosures.

17.4 Data Retention Policy

NGTC strictly adheres to a data retention policy that defines the duration for which personal data is retained. The policy considers the purpose for which data was collected and any statutory obligations. Personal data is not retained beyond the necessary period, minimising the risk of excessive data storage.

17.5 Secure Disposal of Data

NGTC's data disposal procedures align with the GDPR's principle of appropriate data processing. Personal data that has reached its retention date is securely destroyed. Physical records are shredded and disposed of as confidential waste, and digital storage media are securely erased using approved methods before disposal.

17.6 Data Destruction Audit Trail

NGTC maintains an audit trail for data destruction activities. This trail includes records of what data was destroyed, when it was destroyed, and by whom. This documentation ensures accountability and transparency in data disposal processes.

18. Destruction of Personal Data and GDPR Compliance

18.1 Data Disposal Procedures

NGTC's data disposal procedures are meticulously designed to align with GDPR's requirements. Data that is no longer necessary is disposed of promptly and securely to prevent unauthorised access or data breaches.

18.2 Destruction Methods

Personal data is destroyed using approved methods that guarantee the irretrievable removal of information. Physical records are shredded using cross-cut shredders, and digital storage media undergo secure data erasure techniques that render data recovery virtually impossible.

18.3 Data Destruction Verification

NGTC verifies the successful destruction of personal data through validation processes. This verification confirms that the data has been effectively removed and that no remnants remain that could compromise data privacy.

18.4 Documentation of Destruction

NGTC maintains comprehensive records of data destruction activities. These records include details such as the date of destruction, the type of data destroyed, and the methods used. Documentation ensures compliance with GDPR's accountability principle and aids in auditing processes.

18.5 Continuous Improvement

NGTC's commitment to GDPR compliance extends to continuous improvement of data destruction practices. Feedback from audits, incident reports, and regulatory changes inform updates to data disposal methods and procedures, enhancing overall data protection.

18.6 Data Subject Rights and Data Destruction

NGTC recognises that effective data destruction plays a crucial role in respecting data subject rights. By securely disposing of personal data, NGTC ensures that individuals' data is no longer accessible or used beyond its intended purpose, aligning with GDPR's principles of data minimisation and accuracy.

19. Use of Removable Media and GDPR Compliance

19.1 Removable Media Usage Policy

NGTC maintains a stringent stance on the use of removable media to uphold compliance with the General Data Protection Regulation (GDPR). In alignment with data security principles and the safeguarding of personal data, NGTC strictly prohibits the use of removable media within its operations.

19.2 No Use of Removable Media

NGTC does not permit the use of removable media, including USB drives, external hard drives, and other portable storage devices, within its infrastructure. This prohibition extends to all employees, contractors, and personnel who interact with NGTC's systems and data.

19.3 Disciplinary Offence

The use of removable media is considered a severe breach of NGTC's data security policies and GDPR compliance. Engaging in the unauthorised use of removable media, attempting to transfer data to or from such devices, or any related actions are considered a disciplinary offence.

19.4 Data Security and Compliance Priority

NGTC's firm stance against the use of removable media underscores its commitment to data security and GDPR compliance. This policy is in place to prevent the risk of data breaches, unauthorised data transfers, and potential exposure of personal data to external entities.

19.5 Secure Data Transfer Alternatives

To ensure secure data transfer and sharing, NGTC employs alternative methods that adhere to its data security policies. Encrypted file sharing platforms, secure network connections, and controlled access protocols are used to facilitate data exchange while maintaining GDPR compliance.

19.6 Continuous Awareness and Training

NGTC places emphasis on raising awareness among its employees and personnel about the risks associated with removable media usage. Regular training programs inform individuals about the potential consequences of violating the no-removable-media policy and reinforce the importance of compliance.

20. Information Incident Management and GDPR Compliance

20.1 Incident Management Framework

NGTC places paramount importance on effective information incident management to ensure compliance with the General Data Protection Regulation (GDPR). An incident management framework is established to promptly identify, assess, and mitigate any incidents that may compromise the security of personal data.

20.2 Incident Identification

NGTC maintains vigilant monitoring and detection systems to identify potential information incidents. These incidents encompass data breaches, unauthorised access attempts, malware infections, and any activities that pose a risk to the confidentiality, integrity, or availability of personal data.

20.3 Incident Reporting

All employees, contractors, and stakeholders are required to promptly report any suspected or confirmed information incidents to NGTC's designated incident response team. This proactive reporting ensures rapid incident assessment and mitigation.

20.4 Incident Assessment

Upon receiving an incident report, NGTC's incident response team, led by the DPO, conducts a thorough assessment to determine the scope, impact, and severity of the incident. This assessment aids in devising an appropriate response strategy and allocating necessary resources.

20.5 Incident Response

NGTC follows a predefined incident response plan that outlines the steps to be taken in case of an information incident. This plan includes measures to contain the incident, mitigate its impact, and restore normal operations while ensuring GDPR compliance and data subject rights.

20.6 Data Breach Notification

In the event of a personal data breach, NGTC adheres to GDPR's data breach notification requirements. Affected data subjects and relevant authorities are promptly notified, providing transparent information about the nature of the breach, the compromised data, and the mitigation steps taken.

20.7 Documentation and Reporting

All information incidents, responses, and outcomes are thoroughly documented. This documentation aids in post incident analysis, compliance reporting, and continuous improvement of NGTC's incident management processes.

20.8 Incident Analysis and Lessons Learned

Following the resolution of an information incident, NGTC conducts a detailed analysis to identify the root causes and contributing factors. Lessons learned from the incident are used to enhance NGTC's security posture, refine incident response procedures, and prevent future occurrences.

20.9 Data Subject Rights and Incident Management

NGTC's commitment to effective incident management aligns with data subject rights outlined in GDPR. By promptly addressing and mitigating incidents, NGTC ensures the protection of individuals' personal data and the safeguarding of their privacy rights.

20.10 Continuous Enhancement

NGTC's information incident management process undergoes continuous enhancement. Feedback, incident trends, and regulatory changes inform updates to incident response plans, technology investments, and training programs to maintain GDPR compliance and data security.