Funded by Department for Education

SKILLS FOR LIFE

SUPPORTED BY MAYOR OF LONDON

HOLT GREEN TRAINING

Holt Green Training Ltd

DATA PROTECTION/GDPR/PRIVACY POLICY

2024-2025

Policy Statement

Holt Green Training Ltd is committed to a policy of protecting the rights and privacy of individuals (including learners, staff, and others) in accordance with the Data Protection Act 2018 and the General Data Protection Regulations (GDPR). The company needs to process certain information about its staff, learners, and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The policy applies to all staff and learners of the company. Any breach of the Data Protection Act 1998, the GDPR or the Training Company Data Protection Policy is considered to be an offence and in that event, HGT disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the company, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments/sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

Background to the Data Protection Act 2018

The Data Protection Act 2018 replaced the Data Protection Act 1984, and the General Data Protection Regulation, which replaced the 1995 Data Protection Directive, came into force in March 2018. The purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

Article 5 of the GDPR requires that personal data shall be:

"processed lawfully, fairly and in a transparent manner in relation to individuals; collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Definitions

Personal Data

Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, and ID Number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive Data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Data Controller

Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject

Any living individual who is the subject of personal data held by an organisation.

Processing

Any operation related to organisation, retrieval, disclosure, and deletion of data includes Obtaining and recording data accessing, altering, adding to, merging or deleting data.

Third Party

Any individual/organisation other than the data subject, the data controller (Training Company) or its agents.

Relevant Filing System

Any paper filing system or other manual filing system, which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Responsibilities of the Data Protection Act

- The company as a body corporate is the data controller under the new Act.
- Compliance with data protection legislation is the responsibility of all members of the company who process personal information.
- Members of the company are responsible for ensuring that any personal data supplied to the company are accurate and up to date.

Data Protection Principles

All processing of personal data must be done in accordance with the eight data protection principles.

1. Personal data shall be processed fairly and lawfully.

Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

2. Personal data shall be obtained for specified and lawful purposes and not processed in a manner incompatible with those purposes.

Data obtained for specified purposes must not be used for a purpose that differs from those.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.

Information which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

4. Personal data shall be accurate and, where necessary, kept up to date.

Data, kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume accuracy. It

is the responsibility of individuals to ensure that data held by the Training Company is accurate and up to date Completion of an appropriate registration or application form etc. will be taken, as an indication that the data contained therein is accurate. Individuals should notify the Training Company of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Training Company to ensure that any notification regarding change of circumstances is noted and acted upon.

5. Personal data shall be kept only for as long as necessary. (See Section 12 on Retention and Disposal of Data)

6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act. (See Section 7 on Data Subjects Rights).

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data. (See Section 9 on Security of Data).

8. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Data must not be transferred outside of the European Economic Area (EEA) - the EU Member States together with Iceland, Liechtenstein, and Norway - without the explicit consent of the individual. Members of the Training Company should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

Data Subject Rights

Data Subjects have the following rights regarding data processing, and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision making processes that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process. - To sue for compensation if they suffer damage by any contravention of the Act. - To take action to rectify, block, erase or destroy inaccurate data.
- To request the Commissioner to assess whether any provision of the Act has been contravened.

Consent

Wherever possible, personal data or sensitive data should not be obtained, held, used, or disclosed unless the individual has given consent. The company understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord.

Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and sensitive data is obtained routinely by the company (e.g. when a student signs a registration form or when a new member of staff signs a contract of employment). Any company forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data is to be published on the Internet as such data can be accessed from all over the globe. Therefore, not gaining consent could contravene the eighth data protection principle.

If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

If any member of the company is in any doubt about these matters, they should consult the Operations Manager.

Security of Data

All staff are responsible for ensuring that any personal data (on others), which they hold, are kept securely and that they are not disclosed to any unauthorised third party (see Section 11 on Disclosure of Data for more detail).

All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- - In a lockable room with controlled access, or
- - In a locked drawer or filing cabinet, or
- - If computerised, password protected, or
- -Kept on disks which are themselves kept securely.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screensavers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff and learners who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and learners should take particular care when processing personal data at home or in other locations outside the Training Centre.

Rights of Access to Data

Members of the company have the right to access any personal data, which are held by the Training Company in electronic format and manual records, which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the company about that person. Any individual who wishes to exercise this right should apply in writing to the Operations Manager. The company reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee. In order to respond efficiently to subject access requests the company needs to have in place appropriate records management practices.

Disclosure of Data

The company must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police. All staff and learners should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of company business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the company concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. The individual has given their consent (e.g. a student/member of staff has consented to the company corresponding with a named third party).

2. Where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other company employees if it is clear that those members of staff require the information to enable them to perform their jobs).

3. Where the institution is legally obliged to disclose the data (e.g. HESA and HESES returns, ethnic minority and disability monitoring).

4. Where disclosure of data is required for the performance of a contract (e.g. informing a student's LEA or sponsor of course changes/withdrawal etc.).

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- - To safeguard national security.
- - Prevention or detection of crime including the apprehension or prosecution of offenders.
- - Assessment or collection of tax duty.
- - Discharge of regulatory functions (includes health, safety, and welfare of persons at work).
- - To prevent serious harm to a third party.
- - To protect the vital interests of the individual, this refers to life and death situations.

When members of staff receive enquiries as to whether a named individual is a member of the company, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the company may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, the company may offer to do on of the following:

- Pass a message to the data subject asking them to contact the enquirer.
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of the Training Company" to avoid confirming their membership of their presence in or their absence from the institution.

Retention and Disposal of Data

The Training Company discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and learners. However, once a member of staff or student has left the institution, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

Learners

In general, electronic student records containing information about individual learners are kept indefinitely and information would typically include name and address on entry and completion, programmes taken, examination results, awards obtained.

Departments should regularly review the personal files of individual learners in accordance with the company's Records Retention Schedule.

Staff

In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by the Personnel Department for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc. will be retained for the statutory time period (between 3 and 6 years).

Departments should regularly review the personal files of individual staff members in accordance with the company's Records Retention Schedule.

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for12 months from the interview date. Personnel may keep a record of names of individuals that have applied for, be short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

Publication of Company Information

It is recognised that there might be occasions when a member of staff, a student, or other member of the company, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the company should comply with the request and ensure that appropriate action is taken.

Direct Marketing

Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (e.g. an opt-out box on a form).

Information retention policy

The Education and Skills Funding Agency (ESFA) and the Greater Manchester Combined Authority (GMCA) have specific guidelines for information retention within their respective domains. While I can provide general recommendations based on commonly followed practices, it's important to consult the ESFA and GMCA's specific guidelines and legal professionals to ensure compliance with their requirements. Here are some common categories of information and suggested retention periods based on general best practices:

Financial Records:

- Financial transactions, including invoices, receipts, and payment records: Retain for a minimum of six years as per tax and financial regulations.
- Financial statements, budgets, and financial reports: Retain for a minimum of seven years for auditing and financial reporting purposes.

Employee Records:

- Employment contracts and agreements: Retain for the duration of employment and a reasonable period afterward, typically up to six years.
- Payroll records, including salary information and tax records: Retain for a minimum of six years as required by tax and employment laws.
- Disciplinary and grievance records: Retain for a reasonable period to address any employment-related issues or potential legal claims.

Student Records:

- Admission and enrollment records: Retain for a minimum of six years after the student leaves the educational institution, as per ESFA guidelines.
- Attendance registers: Retain for a minimum of three years after the student leaves the institution, as per ESFA guidelines.
- Exam and assessment results: Retain for a minimum of three years after the student leaves the institution, as per ESFA guidelines.

Public Records and Documents:

- Policy documents, governance records, and decision-making records: Retain indefinitely or as specified by applicable legislation or governance guidelines.
- Meeting minutes and agendas: Retain for a reasonable period, typically six years, to demonstrate transparency and decision-making processes.

Contracts and Procurement:

- Contract documents, agreements, and tenders: Retain for the duration of the contract term and a reasonable period afterward, typically up to six years.

Health and Safety Records:

- Incident reports, accident records, and risk assessments: Retain for a reasonable period, typically five to ten years, to address any health and safety-related inquiries or potential legal claims.

We review the specific guidance provided by the ESFA, GMCA, any relevant authorities, and consult legal professionals to ensure compliance with their retention requirements. Additionally, regularly assess and update your retention schedule based on changes in regulations or specific circumstances affecting your organisation.

Recruitment data policy

At Holt Green Training, we prioritise the importance of data management and the safeguarding of sensitive information. As part of our commitment to maintaining a secure and trustworthy environment, we implement thorough pre-employment screening processes for all new employees. These screening procedures are designed to ensure that individuals joining our organisation possess the necessary qualifications, integrity, and professionalism required to handle confidential data.

Our data management pre-employment screening encompasses various aspects, including but not limited to background checks, reference verification, and identity validation. By conducting these screenings, we strive to mitigate potential risks associated with data breaches, unauthorised access, and unethical practices. This process allows us to maintain the highest standards of confidentiality and protect the information entrusted to us by our clients, employees, and stakeholders.

In addition to our comprehensive screening protocols, we adhere to excellent industry standards in data management. Our policies and procedures are designed to align with industry best practices and comply with relevant laws and regulations, including the General Data Protection Regulation (GDPR) and other applicable data protection legislation. We continuously monitor and update our practices to ensure ongoing compliance and to adapt to evolving security threats and technological advancements.

We recognize that data privacy and security are vital concerns for our stakeholders. Therefore, we strive to foster a culture of awareness and accountability within our organisation. Our employees undergo regular training and awareness programs to promote a strong understanding of their roles and responsibilities in maintaining data privacy and adhering to our stringent data management policies.

By implementing robust pre-employment screening processes and adhering to excellent industry standards, Holt Green Training demonstrates its unwavering commitment to protecting the confidentiality, integrity, and availability of data. We understand that data is a valuable asset, and we take all necessary measures to safeguard it against unauthorised access, loss, or misuse.

If you have any questions or concerns regarding our data management pre-employment screening or our commitment to industry standards, please do not hesitate to contact us.

User induction plays a crucial role in ensuring that individuals within an organisation understand their responsibilities regarding data protection. As an industry expert, I recommend the following best practices for user induction and data protection responsibilities:

Comprehensive Training: Provide comprehensive training sessions to all users, including employees, contractors, and third-party vendors, regarding data protection policies, procedures, and best practices. The training should cover topics such as data classification, secure handling of sensitive information, data access controls, and incident reporting.
Clear Policies and Guidelines: Develop clear and concise data protection policies and guidelines that outline the expectations and responsibilities of users. These documents should address data handling, confidentiality, consent, data retention, and data disposal. Make these policies easily accessible and ensure that users are aware of their existence and importance.
Role-Specific Training: Tailor the induction training to the specific roles and responsibilities of different user groups within the organisation. Different roles may have different access privileges, data responsibilities, and compliance requirements. Providing role-specific training helps users understand how data protection applies to their specific tasks and functions.
Regular Updates and Refreshers: Conduct regular training updates and refreshers to ensure that users stay informed about evolving data protection practices, new regulations, and emerging security threats. Reinforce the importance of data protection through periodic reminders, workshops, and awareness campaigns.
Incident Reporting and Response: Educate users on the importance of timely and accurate reporting of data breaches, security incidents, and suspicious activities. Establish clear procedures for incident reporting, escalation, and response. Encourage a culture of accountability and transparency to promote swift action and minimise potential damages.
Data Minimization and Need-to-Know Principle: Emphasise the principle of data minimization and the need-to-know basis for accessing and handling sensitive information. Users should be trained to only collect, process, and retain data that is necessary for their specific job functions, and to adhere to the principle of least privilege when granting access rights.
Regular Assessments and Audits: Conduct regular assessments and audits to evaluate user compliance with data protection policies and procedures. This can include reviewing access logs, performing security assessments, and conducting spot checks. Identify any gaps or areas of improvement and provide additional training or support as needed.
Ongoing Communication: Maintain open lines of communication with users to address any questions, concerns, or clarifications

regarding data protection responsibilities. Encourage a culture of continuous learning and improvement by fostering a supportive environment where users feel comfortable seeking guidance and reporting potential issues.

By following these best practices for user induction and data protection responsibilities, organisations can cultivate a culture of data privacy and security awareness, ensuring that users are equipped with the knowledge and skills to protect sensitive information effectively.

Onsite Work Policy - Home and Mobile Work Prohibition

Policy Statement:

At Holt Green Training, we prioritise the security, confidentiality, and integrity of our information assets. To ensure the highest level of data protection and maintain a controlled working environment, this policy strictly prohibits home and mobile work for all employees, contractors, and third-party vendors. All work activities must be conducted exclusively on-site within designated company premises.

Policy Guidelines:

Onsite Work Requirement:
a. All employees, contractors, and third-party vendors must perform their work duties solely within the physical premises designated by Holt Green Training.
b. Remote work, including work from home, telecommuting, or mobile work, is strictly prohibited without prior written approval from the management.

Data Security and Confidentiality:
a. Onsite work facilitates better control over data security measures, including physical security, access controls, and network infrastructure.
b. By maintaining a centralised work environment, we can ensure the confidentiality and integrity of sensitive information and minimise the risk of data breaches or unauthorised access.

Compliance with Policies and Procedures:
a. All employees, contractors, and third-party vendors must comply with the organisation's information security policies, procedures, and best practices while working on-site.
b. By working exclusively on-site, individuals can receive timely guidance, support, and supervision from the relevant departments, fostering a cohesive and secure work environment.

Exception Process:
a. Requests for remote work due to exceptional circumstances (e.g., medical reasons, extreme weather conditions) must be submitted in writing to the management for consideration.
b. Management will review exception requests on a case-by-case basis, weighing the individual circumstances against the organisation's security requirements.
c. Approved exceptions will be subject to specific terms and conditions outlined in a separate agreement.

Policy Violations:
a. Any violation of this policy may result in disciplinary action, up to and including termination of employment or contract termination.
b. Suspected policy violations should be reported promptly to the appropriate department or the designated contact person.

Policy Review:

This policy will be reviewed on an annual basis or as deemed necessary by the management to ensure its effectiveness and alignment with changing business requirements, industry standards, and legal regulations.

Acknowledgment:

By continuing employment or engagement with Holt Green Training, all employees, contractors, and third-party vendors acknowledge their

understanding and compliance with this policy.

For any questions or clarifications regarding this policy, please contact the Data Protection Officer at Holt Green Training..

Note: This policy is a sample and should be customised to fit the specific requirements and legal obligations of Holt Green Training. It is essential to consult with legal professionals to ensure compliance with applicable laws and regulations.

Information Incident Management

Effective incident management is critical for organisations to respond swiftly and effectively to information security incidents. By following best practices, organisations can minimise the impact of incidents, protect sensitive data, and maintain stakeholder trust. Here are key elements of information incident management best practices:

Incident Response Plan:

- Develop a comprehensive incident response plan (IRP) that outlines the step-by-step procedures to follow in the event of an incident.
- Assign clear roles and responsibilities to designated individuals or teams within the organisation.
- Include contact information for key stakeholders, such as IT personnel, legal advisors, senior management, and relevant regulatory authorities.

Incident Identification and Reporting:

- Implement robust monitoring and detection systems to identify potential incidents promptly.
- Establish clear reporting channels and encourage employees to report any suspicious activities or incidents they encounter.
- Maintain incident reporting mechanisms that allow for anonymous reporting, ensuring a safe and secure means of communication.

Incident Categorization and Prioritization:

- Develop a system for categorising and prioritising incidents based on their severity, impact, and potential harm to the organisation.
- Establish criteria for incident classification, such as the level of confidentiality, integrity, and availability of compromised data.
- Prioritise incidents based on the potential damage, legal or regulatory requirements, and the organisation's risk appetite.

Incident Response and Containment:

- Activate the incident response plan promptly upon detection or notification of an incident.
- Isolate affected systems or networks to prevent further spread of the incident and limit the potential impact.
- Gather and preserve evidence related to the incident for potential legal or forensic analysis.

Communication and Stakeholder Management:

- Establish a clear communication protocol to keep all relevant stakeholders informed throughout the incident response process.
- Assign a designated spokesperson to manage external communications and coordinate with affected parties, such as customers, partners, and regulatory bodies.
- Provide timely and accurate updates on the incident's status, impact, and remediation efforts.

Investigation and Root Cause Analysis:

- Conduct a thorough investigation to determine the root cause of the incident and identify any vulnerabilities or weaknesses in existing security controls.
- Document the findings and recommendations for improving security measures to prevent similar incidents in the future.
- Implement corrective actions to address identified gaps and enhance the organisation's overall security posture.

Learning and Continuous Improvement:

- Conduct post-incident reviews and lessons learned sessions to identify areas for improvement in incident response processes and procedures.
- Update the incident response plan and other relevant documentation based on the insights gained from incident analysis.
- Provide regular training and awareness programs to educate employees about incident management best practices and their roles in incident response.

Regular Testing and Exercises:

- Conduct regular incident response exercises and simulations to test the effectiveness of the incident response plan.
- Evaluate the organisation's ability to detect, respond, and recover from different types of incidents.
- Identify areas for improvement and refine the incident response plan based on the outcomes of these exercises.

Remember, each organisation's incident management process should be tailored to its specific industry, size, and regulatory requirements. It is crucial to consult with legal, IT, and security professionals to ensure compliance with applicable laws and regulations and align incident management practices with the organisation's unique needs.

Storage and Destruction Policy for Holt Green Training Limited

The purpose of this Storage and Destruction Policy is to establish guidelines for the proper storage, retention, and disposal of confidential and sensitive information within Holt Green Training Limited. This policy aims to protect the company's data, maintain compliance with relevant laws and regulations, and mitigate the risk of unauthorised access or data breaches.
Scope This policy applies to all employees, contractors, and third-party vendors who handle, store, or have access to Holt Green Training Limited's information assets.

Information Classification Holt Green Training Limited classifies its information assets into the following categories:

1. **Confidential:** Information that is highly sensitive, proprietary, or subject to legal and contractual obligations. Unauthorised disclosure, alteration, or destruction of confidential information may result in severe consequences for the company.

2. **Internal Use:** Information that is intended for internal use within the organisation and should not be disclosed to external parties without proper authorization.

3. **Public:** Information that is meant for public consumption and does not contain sensitive or confidential data.

Storage Procedures

1. **Physical Storage:**

a. Physical storage areas, such as filing cabinets or secure rooms, should be used for storing physical documents containing confidential or sensitive information.

b. Access to physical storage areas should be restricted to authorised personnel only.

c. Physical documents should be properly labelled and organised to facilitate efficient retrieval and minimise the risk of loss or misplacement.

2. **Digital Storage**:

a. Digital information should be stored on secure servers or cloud-based platforms that provide appropriate security measures.

b. Access to digital storage systems should be restricted to authorised personnel based on the principle of least privilege.

c.. Strong passwords and encryption should be used to protect digital storage systems from unauthorised access.

3. Retention Periods

a. Holt Green Training Limited will establish retention periods for different types of information in compliance with legal and regulatory requirements. b. Information that has reached the end of its retention period should be promptly disposed of as outlined in the destruction procedures below.

Destruction Procedures

1. **Physical Destruction**:

a. Physical documents should be shredded or incinerated using secure methods to prevent unauthorised retrieval.

b. Disposal containers specifically designed for sensitive document destruction should be used.

c. Employees should not dispose of sensitive documents in regular waste bins.

2. **Digital Destruction:**

a. Digital information should be permanently and securely deleted from storage systems.

b. Deleting files from storage devices may not be sufficient, and data erasure or destruction tools should be used to ensure complete elimination.

c. Backup copies containing sensitive information should also be securely deleted.

Training and Awareness Holt Green Training Limited will provide training and awareness programs to employees, contractors, and vendors regarding this Storage and Destruction Policy. Employees should be regularly updated on their responsibilities and best practices for handling, storing, and disposing of confidential and sensitive information.
Monitoring and Compliance The company may conduct periodic audits and reviews to ensure compliance with this policy. Any non-compliance or breaches of the policy should be reported to the appropriate authorities and may result in disciplinary action.
Policy Review This Storage and Destruction Policy will be reviewed periodically to ensure its continued effectiveness and relevance. Changes or updates to the policy will be communicated to all relevant parties.

By adhering to this Storage and Destruction Policy, Holt Green Training Limited aims to safeguard its confidential and sensitive information, protect its reputation, and comply with legal and regulatory obligations.

Personal Data

Paper-Based Transmission

a. Use Envelopes: When transmitting personal data through the postal system, always use envelopes that are opaque and provide adequate protection. Avoid using transparent or flimsy envelopes that could easily be tampered with or allow the contents to be visible.

b. Registered or Certified Mail: Consider using registered or certified mail services that provide tracking and require the recipient's signature upon delivery. This helps ensure that the sensitive information reaches the intended recipient securely.

c. Double-Envelope Method: For highly sensitive personal data, adopt the double-envelope method. Place the document containing personal data in one envelope, seal it, and then place it in a larger envelope for additional protection.

d. Correct Addressing: Verify and double-check the recipient's address to avoid misdelivery or unauthorised access to personal data.

e. Avoid Outsourcing: Whenever possible, avoid outsourcing the transmission of personal data to third-party mailing services. If outsourcing is necessary, ensure that the service provider has appropriate security measures and a proven track record of handling sensitive information.

Electronic Transmission

a. Encryption: Utilise encryption techniques to protect personal data during transmission. Use secure file transfer protocols (SFTP, FTPS) or email encryption (PGP, S/MIME) to ensure that the data remains encrypted while in transit.

b. Secure File Sharing Platforms: When transmitting personal data electronically, consider using secure file sharing platforms that offer encryption, password protection, and access controls. These platforms provide an added layer of security and control over the transmitted data.

c. Password Protection: If transmitting personal data through email or other means that do not provide built-in encryption, protect the data by encrypting it with a strong password. Share the password with the recipient through a separate communication channel (e.g., phone call) to minimise the risk of interception.

d. Data Integrity: Ensure that the transmitted data maintains its integrity during transmission. Implement mechanisms such as checksums or digital signatures to verify that the data has not been tampered with or altered in transit.

e. Avoid Public Networks: When transmitting personal data electronically, avoid using public or unsecured Wi-Fi networks. Use a secure and private network connection to minimise the risk of unauthorised interception.

f. Regular Software Updates: Keep the software and applications used for transmitting personal data up to date with the latest security patches and updates. Outdated software may have vulnerabilities that could be exploited by attackers.

g. Use Virtual Private Networks (VPNs): If transmitting personal data over the internet, consider using VPNs to establish secure and encrypted connections between the sender and the recipient. VPNs add an extra layer of protection by encrypting all data traffic between the two endpoints.

Employee Awareness and Training

a. Provide Training: Educate employees on the proper procedures and best practices for securely transmitting personal data, both on paper and electronically. Ensure they understand the importance of confidentiality, the risks involved, and the measures in place to protect personal data during transmission.

b. Confidentiality Agreements: Require employees who handle personal data to sign confidentiality agreements, reinforcing their responsibility to safeguard the information during transmission and at all times.

c. Regular Reminders: Conduct periodic reminders and updates to reinforce security practices and keep employees vigilant about secure transmission methods.

Securities Allocation of User Access Privileges - Two-Person Approval Approach

At Holt Green Training, we recognise the importance of maintaining a robust system for managing user access privileges to safeguard sensitive data and protect against unauthorised access. To ensure a stringent control mechanism, we adopt a two-person approval approach, requiring both the Data Protection Officer (DPO) and a Senior Manager to sign off on any and all staff access requests.

Policy Guidelines:

User Access Request Process:

a. All user access requests must be submitted through an official access request form or system.
b. The access request form should include relevant details such as the employee's name, job title, department, reason for access, and specific permissions required.
c. Access requests should be reviewed and approved by both the DPO and a designated Senior Manager.

Data Protection Officer (DPO) Responsibilities:
a. The DPO is responsible for overseeing data protection and privacy matters within the organisation.
b. The DPO will review access requests to ensure compliance with data protection policies, regulatory requirements, and the principle of least privilege.
c. The DPO will assess the necessity and appropriateness of the requested access privileges based on the employee's job responsibilities.
Senior Manager Responsibilities:
a. A Senior Manager, designated by the organisation, will work alongside the DPO in reviewing and approving access requests.
b. The Senior Manager will provide an additional layer of oversight and accountability to ensure proper authorization of access privileges.
c. The Senior Manager will assess the business justification and need for the requested access privileges in alignment with the organisation's operational requirements.
Approval Process:
a. Access requests will be reviewed independently by both the DPO and the Senior Manager.
b. Both the DPO and the Senior Manager must sign off on the access request before access privileges are granted.
c. If either party identifies concerns or requires additional information, they may request clarification or further documentation before making a final decision.
Access Revocation:
a. Access privileges should be periodically reviewed to ensure ongoing necessity and relevance.
b. If access is no longer required or an employee's role changes, access privileges should be promptly revoked or modified accordingly.
c. The DPO and the Senior Manager will collaborate to review and approve any changes to access privileges.
Documentation and Audit Trail:
a. Maintain a comprehensive record of all access requests, approvals, modifications, and revocations.
b. The access request form or system should capture the date, names of the approving parties, and any relevant comments or justifications.
c. The documentation and audit trail should be available for internal and external audits, demonstrating adherence to the two-person approval approach.

Policy Review:

This policy will be reviewed on an annual basis or as deemed necessary by the organisation's management to ensure its effectiveness, alignment with regulatory requirements, and continuous improvement.

Acknowledgment:

By continuing employment or engagement with Holt Green Training, all employees acknowledge their understanding and compliance with this policy. For any questions or clarifications regarding this policy, please contact the Data Protection Officer at Holt Green Training.

At Holt Green Training, we prioritise the continuity of our business operations and the protection of our data assets. To ensure an effective business continuity management process, we adhere to industry best practices for data protection and leverage Google's robust security measures. This policy outlines our commitment to business continuity and data security, as well as our reliance on Google for secure infrastructure and services.

Policy Guidelines:

Business Continuity Management Process:
a. Establish a comprehensive business continuity management process that encompasses risk assessment, business impact analysis, development of recovery strategies, and ongoing testing and maintenance.
b. Align the process with internationally recognized standards and best practices, such as ISO 22301 or other relevant frameworks.
Data Protection Best Practices:
a. Implement a data protection framework that includes data classification, encryption, access controls, and regular data backups.

b. Adhere to the principle of least privilege, ensuring that access to data and systems is granted based on the specific needs and responsibilities of individuals.
c. Regularly review and update data protection measures to address emerging threats and changes in regulatory requirements.
Use of Google for Robust Security:
a. Leverage Google's robust security infrastructure, services, and technologies to enhance the security and resilience of our business operations and data.
b. Utilise Google Cloud Platform (GCP) for secure hosting and storage of data, taking advantage of Google's advanced data protection and privacy controls.
c. Benefit from Google's extensive investment in security measures, including physical security, network security, encryption, and threat detection capabilities.
Data Governance and Compliance:
a. Establish clear data governance policies and procedures to ensure compliance with relevant laws, regulations, and industry standards.
b. Regularly monitor and assess our data management practices to ensure ongoing compliance and address any identified gaps or vulnerabilities.
Incident Response and Recovery:
a. Develop an incident response and recovery plan that outlines the steps to be taken in the event of a disruption, data breach, or other incidents.
b. Ensure that the plan includes roles and responsibilities, communication protocols, data recovery procedures, and post-incident analysis and improvement processes.
Employee Training and Awareness:
a. Provide regular training and awareness programs to employees on business continuity, data protection, and their roles in maintaining operational resilience.
b. Foster a culture of security awareness and encourage employees to report any potential risks, incidents, or vulnerabilities promptly.
Continuous Improvement: a. Conduct regular reviews, assessments, and testing of the business continuity management process to identify areas for improvement and implement necessary enhancements.
b. Stay updated with emerging best practices, industry trends, and technological advancements to ensure the ongoing effectiveness and relevance of our approach.
Policy Review: This policy will be reviewed on an annual basis or as required by changes in regulatory requirements, industry standards, or organisational needs.

Rules Governing Acceptable Use of Information Assets - Best Practice

Policy Statement:

At Holt Green Training, we recognize the importance of maintaining the security, integrity, and confidentiality of our information assets. This policy establishes guidelines for the acceptable use of information assets to ensure their proper handling, protection, and compliance with applicable laws and regulations. Adherence to these rules is essential to maintain a secure and productive computing environment for all users.

Policy Guidelines:

User Responsibilities:
a. Users must familiarise themselves with and comply with all applicable laws, regulations, and organisational policies governing information assets.
b. Users are responsible for using information assets in a manner that aligns with their job duties and the legitimate needs of the organisation.
c. Users should report any suspected security incidents or violations of this policy to the appropriate authority.
Information Classification:
a. All information assets must be classified based on their sensitivity, value, and criticality to the organisation.
b. Users must understand the classification of information they handle and ensure that appropriate safeguards are in place to protect classified data.
Access Control:

a. Users must only access information assets for which they have been authorised.
b. Users must protect their login credentials and not share them with unauthorised individuals.
c. Users must log out or lock their workstation when leaving it unattended to prevent unauthorised access.

Data Protection:

a. Users must exercise care in handling sensitive information to prevent unauthorised access, disclosure, or alteration.
b. Users should encrypt sensitive data when transmitting it over untrusted networks or storing it on portable devices.
c. Users should adhere to data retention and destruction policies to ensure the secure disposal of information when no longer needed.

Acceptable Use:

a. Users must use information assets for legitimate business purposes and refrain from using them for personal gain or illegal activities.
b. Users should not install unauthorised software, access unauthorised websites, or engage in activities that could compromise the security or integrity of information assets.
c. Users must refrain from sending or accessing offensive, inappropriate, or harassing content.

Intellectual Property and Copyright:

a. Users must respect intellectual property rights and adhere to copyright laws when using software, documents, images, or any other copyrighted material.
b. Users should not engage in unauthorised reproduction, distribution, or modification of copyrighted materials.

Monitoring and Auditing:

a. The organisation reserves the right to monitor and audit information assets and user activities to ensure compliance with this policy and applicable laws. b. Users should have no expectation of privacy when using organisational information assets.

Consequences of Violations:

a. Violations of this policy may result in disciplinary action, up to and including termination of employment or legal action, depending on the severity of the violation and any applicable laws.

Policy Review: This policy will be reviewed periodically to ensure its effectiveness, alignment with legal and regulatory requirements, and relevance to organisational needs.

Acknowledgment:

By continuing employment or engagement with Holt Green Training, all users acknowledge their understanding and compliance with this policy.

Requests must be supported by appropriate paperwork and clearance from the Data Protection officer and one Senior manager.