ELA Training Services

Information Security Policy
Organisational Controls

1st August 2023
V2.0

Contents

Document History

Issue	Issue Date	Author	Revision Notes
1	19th February 2023	MJ	Draft v 0.01 – First Draft
2	20th February 2023	MJ	Draft v0.01 Amends
3	21st February 2023	MJ	Draft v0.01 Amends
4	22nd February 2023	MJ	Draft v0.01 Amends & Layout
5	1st March 2023	MJ	Move from Draft to release V 1.0
6	1 August 2023		Amends V 2.0

Document History

In relation to Personal Identifiable Information (PII) this document sets out the policies and procedures that collectively ensure that effective information security management controls are in place throughout ELA.

This policy encompasses information that is stored in both electronic and paper-based formats or processing systems.

Document Structure

The structure of this document is based broadly on the global information security standard ISO 27001.
There are 25 main sections; each section addresses a specific set of controls related to particular threats, risks, and vulnerabilities. However, with the exception of Information Asset Owners, policy makers and senior management (who must read the document in its entirety and sign off as part of the corporate governance) the document is designed to be read as a reference document (together with the 'Information Security Policy – Technical Controls' and standard governance and control policies of ELA Training Services).
Each section contains one or more policies. A policy is an overall statement of intent and direction.

Most policies in turn have procedures associated with them. These are specific controls and requirements aimed at ensuring the policy is implemented effectively.

Some policies also have standards associated with them. These are essentially specifications (e.g., prescribed settings for a security device) as opposed to the "how to" nature of procedures.

Document Control

ELA's information security policies and procedures are living documents. Reviews will be conducted, at a minimum annually, by the ELA Risk Assurance Team (and if necessary the Data Compliance Manager) to ensure that the policies and procedures are continuing to achieve their purpose as a practical operational framework for ensuring a suitable level of security for ELA, its clients, employers, learners, suppliers and other 3rd Parties.

The ELA Risk Assurance Team (refer to Section 1.22.1 for Information Security Terms of Reference) is responsible for ensuring that the information security policies and procedures continually align with ELA's operational requirements and reflect ELA's overall requirements for effective risk management.

All revisions to the information security policies and procedures must be agreed by the ELA Risk Assurance team.

Security Policy Management

1.1 Management of Information Security Policies

ELAs management team is committed to ensuring that the firms information security policies and procedures accurately reflect ELAs business requirements and are in line with all relevant laws and regulations.

ELAs management will take all necessary steps to ensure compliance with the firm's information security policies and procedures at all times. A Security Threat and Countermeasures Register will be kept comprising a list of all known perceived threats and countermeasures and a target date for the resolution of the non-compliance if appropriate.

1.2 Compliance Review Process

The ELA Risk Assurance Team is responsible for monitoring compliance with the information security policies and procedures.

It is recognised that from time to time operational or commercial imperatives may require a level of departure from the policies and procedures, but all actions must remain within accepted risk tolerance and be legally compliant.

General Data Protection Regulation (GDPR) Introduction

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

The General Data Protection Regulation aims 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 that it is processed with their consent.

1.4 Definitions

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means as well as 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 applies to all controllers that are established in the EU (European Union) who process the personal data of data subjects. It also applies 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.

1.5 Article 4 definitions

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person 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 Law, the controller or the specific criteria for its nomination may be provided for by 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 of personal data relating to that individual.

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 of 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. This can be either a manual paper based or an electronic system.

Responsibilities

1.6 Executive Committee

The Executive Committee are committed to compliance with all relevant laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information is processed in accordance with the General Data Protection Regulation (GDPR). The ELA Head of MIS, Compliance & Admin is the Board representative on ELA Risk Assurance Team.

1.7 Group Risk Assurance Team

The ELA Risk Assurance Team will establish and maintain a Risk Register which shall comprise a list of all perceived threats and countermeasures.

The Risk Register shall be reviewed by the ELA Risk Assurance Team at least once every three months to ensure that suitable progress is being made in identifying threats and recommending the countermeasures to the Executive Committee.

1.8 Operational Management

It is the responsibility of all Managers to familiarise themselves with company procedures and to ensure that all Employees have access to the latest issue which will be stored on the Company SharePoint instance.

1.9 Information Asset Owners

An Information Asset Owner (IAO) must be a member of the senior management team, is a member of the company Risk Assurance Team for the management of personal data within ELA and for ensuring that compliance with this policy in relation to the Information Asset for which they are responsible.

The Information Asset Owners have specific responsibilities in respect of procedures such as the Subject Access Request (SAR) Procedure and are the first point of call for Employees seeking clarification on any aspect of data protection compliance for their specific information asset.

The IAO is responsible for ensuring:

1. Privacy notices are correct and that mechanisms exist to make all data subjects aware of the contents of this notice prior to ELA commencing collection of their data.
2. User access is continually reviewed to prevent unauthorised access.
3. Appropriate arrangements that, where 3rd 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 to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the 3rd party where this is required.
4. All Employees are trained in the importance of collecting accurate data and maintaining it.
5. 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.
6. On at least a quarterly basis, the Information Asset Owner will review the retention dates of all the personal data processed by the systems they are responsible for, 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 deleted/destroyed in line with the Secure Disposal detailed in Information Security Policy – Technical Controls.

7. The asset is properly licensed and only used in accordance with the terms of that licence even if the software is a Software as a Service (SaaS) or provided by a 3rd party supplier/IT partner.
8. ELA responds to requests for rectification from data subjects within one month (Please see Subject Access Procedure). This can be extended to a further two months for complex requests. If ELA decides not to comply with the request, the Information Asset Owner must respond to the data subject to explain their reasoning and inform them of their right to complain to the Information Commissioners Office and seek judicial remedy.

1.10 Employees

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

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

This policy applies to all Employees of ELA and outsourced suppliers & contracted associates. Any breach of this policy will be subject to ELA's disciplinary policy, and the unlawful processing of personal data may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

1.11 3rd Parties and Partners

Partners and any 3rd Parties working with or for ELA, 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 processed by ELA without having first entered into a data confidentiality agreement (3rd party processing contracts), which imposes on the third-party obligations no less onerous than those to which ELA is committed, (and which are required by law), and which gives ELA the right to audit compliance with the agreement.

1.12 Data Subjects

It is the responsibility of the data subject to ensure that data held by ELA 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.

Data Protection Principles

All processing of personal data is conducted in accordance with the data protection principles as described below (and set out in Article 5 of the GDPR). ELA's policies and procedures are designed to ensure compliance with the principles.

The Six Data Protection Principles state that personal data:

1. Must be processed lawfully, fairly, and transparently.
2. Can only be collected for specific, explicit, and legitimate purposes.
3. Must be adequate, relevant, and limited to what is necessary for processing.
4. Must be accurate and kept up to date with every effort to erase or rectify without delay.
5. Must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
6. Must be processed in a manner that ensures the appropriate security.

Whilst not written as a principle, ELA must be able to demonstrate ***accountability*** through the application of this Information Security Policy by '***Default and by design'.***

1.13 Lawfully, fairly, and transparently

Lawful – ELA has identified (from one of the six listed below) a lawful basis for processing personal data before data processing begins. Further detail is contained within the Data Protection Impact Assessment.

The legal basis for processing includes:

1. Consent
2. Contractual obligation
3. Legal obligation
4. Vital interests
5. Public interest
6. Legitimate interests

Fairly – In order for processing to be fair ELA makes certain information available to its data subjects as required. This applies whether the personal data was obtained directly from the data subjects or from other sources. The data subject is notified via a privacy notice.

Transparently – ELA is committed to communicating to its data subject in an intelligible form using clear and plain language. Privacy notices are used to provide relevant information (as described below) and additionally provides the data subject with the ability to provide consent.

1.13.1 Privacy Notices Contents

The specific information that is provided to the data subject includes (as a minimum):

- The identity and the contact details of the controller and, if any, of the controller's representative,
- The contact details of the Information Asset Owner,
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing,
- The period for which the personal data will be stored,
- The existence of the rights to request access, rectification, erasure or to object to the processing,
- The categories of personal data concerned,
- The recipients or categories of recipients of the personal data, where applicable,
- 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,
- Any further information necessary to guarantee fair processing,
- The right to lodge a complaint with the Information Commissioners Office.

1.14 Collected for specific, explicit, and legitimate purposes.

ELA only uses data for specified purposes and does not use data for a purpose that differs from those formally notified to the supervisory authority as part of ELA's GDPR register of processing.
The Privacy Procedure sets out the relevant procedures.

1.15 Adequate, relevant, and limited to what is necessary.

The Information Asset Owner is responsible for ensuring that ELA does not collect information that is not strictly necessary for the purpose for which it is obtained under GDPR guidelines.

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

The Information Asset Owner 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.

1.16 Accurate and kept up to date.

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

Employees are required to notify the IAO of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of ELA to ensure that any notification regarding change of circumstances is recorded and acted upon.

1.17 Kept only as long as is necessary.

Where personal data is retained beyond the processing date, suitable methods will be employed (for example minimisation, encryption and/or pseudonymisation) in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the Retention of Records Procedure (please refer to section 1.36) and, once its retention date is passed, it must be securely destroyed in accordance with the retention of data section. Cross reference to the ELA Data Protection Policy and Document retention policy will help determine contractual and legislative document retention dates.

The IAO 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 documented and stored appropriately.

1.18 Ensures the appropriate security.

The Head of MIS, Compliance & Admin or the Data Compliance Manager will carry out a risk assessment taking into account all the circumstances of ELA's controlling or processing operations.

In determining appropriateness, The Head of MIS, Compliance & Admin or the Data Compliance Manager should also consider the extent of possible damage or loss that might be caused to individuals (e.g. Employees or Clients) if a security breach occurs, the effect of any security breach on ELA itself, and any likely reputational damage including the possible loss of client trust.

When assessing appropriate measures, the Head of MIS, Compliance & Admin or the Data Compliance Manager will consider the following:

Physical Controls for example:

- Door access systems or lockable doors
- lockable filing cabinets
- staffed reception areas)

Technical Controls (Please refer to Information Security – Technical Controls Policy).

- Password protection
- Automatic locking of idle terminals/screens/devices
- Removal of access rights for USB and other memory media.
- Virus checking software and firewalls.
- Role-based access rights / Permissions including those assigned to temporary Employees.
- Encryption of devices that leave ELAs premises such as laptops/mobile devices.
- Security of local (LAN) and wide area networks (WAN)/Cloud

Managerial Controls

- Policies
- Processes
- Employee education/training
- Measures that consider the reliability of employees (e.g., obtaining references etc.)
- Data classification
- Adoption of a clear desk policy
- Privacy enhancing technologies such as pseudonymisation and anonymization.
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

1.19 Accountability

The GDPR legislation includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires that ELA to demonstrate compliance with the principles.

ELA demonstrates compliance with the six data protection principles listed above by implementing this Information Security Policy, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, Data Protection Impact Assessments, breach notification procedures and incident response plans.

In summary, ELA has data protection at its core by default and by design.

Privacy Procedure

ELA identifies the legal basis for processing personal data before any processing operations take place by clearly establishing, defining, and documenting:

The specific purpose of processing the personal data and the legal basis to process the data under:

- Consent obtained from the data subject.
- Performance of a contract where the data subject is a party.
- Legal obligation that ELA is required to meet.
- Protect the vital interests of the data subject, including the protection of rights and freedoms.
- Official authority of ELA or to carry out the processing that is in the public interest.
- Necessary for the legitimate interests of the data controller or third party, unless the processing is overridden by the vital interests, including rights and freedoms.
- National law.

Any special categories of personal data processed and the legal basis to process the data under:

- Explicit consent obtained from the data subject.
- Necessary for employment rights or obligations.
- Protect the vital interests of the data subject, including the protection of rights and freedoms.
- Necessary for the legitimate activities with appropriate safeguards.
- Personal data made public by the data subject.
- Legal claims.

- Substantial public interest.
- Preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, provision of health or social care treatment, or management of health and social care systems and services, under the basis that appropriate contracts with health professionals and safeguards are in place.
- Public health, ensuring appropriate safeguards are in place for the protection of rights and freedoms of the data subject, or professional secrecy.
- National laws in terms of processing genetic, biometric or health data.

ELA records this information in line with its data protection impact assessment and data inventory.

1.20 Privacy notices

When personal data collected from data subject with consent:

ELA is transparent in its processing of personal data and provides the data subject with the following:

- ELA's identity and contact details of the Information Asset Owner and any data protection representatives.
- The purpose(s), including legal basis, for the intended processing of personal data.
- Where relevant, ELA's legitimate interests that provide the legal basis for the processing.
- Potential recipients of personal data.
- Any information regarding the intention to disclose personal data to third parties and whether it is physically transferred outside the UK/EU. In such circumstances, ELA will provide information on the safeguards in place and how the data subject can also obtain a copy of these safeguards.
- Even though ELA is a UK registered Company If ELA was based outside of the EU and the data subject resides within it (the EU), ELA provides the data subject with contact details of a data protection representative in the EU.
- Any information on website technologies used to collect personal data about the data subject.
- Any other information required to demonstrate that the processing is fair and transparent. (For example, retention period, right to lodge a complaint, right to withdraw consent and whether any decisions are made automatically as a result of the processing).

All information provided to the data subject is in an easily accessible format, using clear and plain language, especially for personal data addressed to a child.

When data is contractually required for processing, ELA processes data without consent in order to fulfil contractual obligations (such as bank details to process salaries, postal address in order to supply products and services, etc.).

When personal data has been obtained from a source other than the data subject ELA makes clear the types of information collected as well as the source of the personal data (publicly accessible sources) and provides the data subject with:

- ELA's (data controller) identity, and contact details of the Information Asset Owner and any data protection representatives.
- The purpose(s), including legal basis, for the intended processing of personal data.
- Categories of personal data.
- Potential recipients of personal data.
- Any information regarding disclosing personal data to third parties and whether it is transferred outside the EU – ELA will provide information on the safeguards in place and how the data subject can also obtain a copy of these safeguards.
- Any other information required to demonstrate that the processing is fair and transparent.

The above does not apply:

- If the data subject already has the information;(Evidenced)
- If the provision of the above information proves impossible or would involve an excessive effort.
- If obtaining or disclosure of personal data is expressly identified by Member State law; or
- If personal data must remain confidential subject to an obligation of professional secrecy regulated by Member State law, including a statutory obligation of secrecy.

Data Subjects' Rights

Article 12 through to 23 of the GDPR detail the rights of the data subject, these are summarised below:

- To make Subject Access Requests (SAR) 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-taking process that will significantly affect them.
- To not 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 GDPR legislation.
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- To request the Information Commissioners Office to assess whether any provision of the GDPR legislation has been contravened.
- 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.
- To object to any automated profiling that is occurring without consent.

ELA ensures that data subjects may exercise these rights:

- Data subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how ELA will ensure that its response to the data access request complies with the requirements of the GDPR legislation.
- Data subjects have the right to complain to ELA 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 Customer Complaints Procedure.

Data Subjects' Consent

ELA 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 and ELA ensures this is achieved as easily as it was for the data subject to grant consent.

ELA 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 on the basis of misleading information will not be a valid basis for processing.

There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Information Asset Owner must be able to demonstrate that consent was obtained for the processing operation.

For sensitive data (Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade union membership, Genetic data, Biometric data). The explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists (Contractual basis exist for Individual Learner Records & forms)

Where ELA provides online services to children, parental or custodial authorisation must be obtained. This requirement currently applies to children under the age of 16.

Consent procedure

ELA provides a clear privacy and fair processing notice wherever personal data is collected (refer to Section 1.20) ensuring that consent is informed, and that the data subject is informed of their rights in relation to their personal data.

ELA demonstrates Data Subject(s) consent.

- to the processing of his or her personal data for one or more specific purposes.
- is clearly distinguishable from any other matter relating to the data subject.
- is intelligible and accessible using clear and plain language.

ELA demonstrates Data subject(s) are informed of their right to withdraw consent before giving consent.

Processing of data is limited to that stated in the contract, bound by the explicit consent given by the data subject.

Where processing relates to a child under 16 years old, ELA demonstrates that consent has been provided by the person who is the holder of parental responsibility over the child.

ELA demonstrates reasonable efforts have been made to verify the age of the child and establish the authenticity of the parental responsibility.

Subject Access Procedure

Subject Access Requests are made using the Subject Access Request Record. See Appendix A.

The data subject provides ELA with evidence of their identity as the request can be written or made verbally.

The data subject specifies to ELA specific set of data held by ELA on their subject access request SAR). The data subject can request all data held on them.

ELA records the date that the identification checks were conducted, and the specification of the data sought.

ELA provides the requested information to the data subject within one month from this recorded date.

Once received and qualified, the subject access request (SAR) application is immediately forwarded to the Information Asset Owner, who will ensure that the requested data is collected within the specified time frame (default of one calendar month).

The Information Asset Owner reviews all documents that have been provided to identify whether any third parties are present in it, and either removes the identifying third party information from the documentation or obtains written consent from the third party for their identity to be revealed.

If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided:

- National security
- Crime and taxation
- Health
- Education
- Social Work
- Regulatory activity
- Journalism, literature, and art
- Research history, and statistics
- Publicly available information
- Corporate finance
- Examination marks
- Examinations scripts
- Domestic processing
- Confidential references
- Judicial appointments, honours, and dignities
- Crown of ministerial appointments
- Management forecasts
- Negotiations
- Legal advice and proceedings
- Self-incrimination
- Human fertilization and embryology
- Adoption records
- Special educational needs
- Parental records and reports

In the event that a data subject requests ELA to provide them with the personal data stored by the controller/processor, then ELA will provide the data subject with the requested information in electronic format, unless otherwise specified.

In the event that a data subject requests what personal data is being processed then ELA provides the data subject with the following information from the point of data collection:

- Purpose of the processing
- Categories of personal data
- Recipient(s) of the information, including recipients in third countries or international organisations.
- How long the personal data will be stored.
- The data subject's right to request rectification or erasure, restriction, or objection, relative to their personal data being processed.
    - ELA removes personal data from systems and processing operations as soon as a request for erasure has been submitted by the data subject.
    - ELA contacts and communicates with other organisations, where the personal data of the data subject is being processed, to cease processing information at the request of the data subject.
    - In the event that the data subject has withdrawn consent ELA takes appropriate measures without undue delay.

- Inform the data subject of their right to lodge a complaint with the Information Commissioners Office and a method to do so.
- Information on the source of the personal data if it hasn't been collected from the data subject.
- Inform the data subject of any automated decision-making.
- If and where personal data has been transferred and information on any safeguards in place.

Disclosure of data

ELA must ensure that personal data is not disclosed to unauthorised 3rd 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 3rd Party and will be required to attend specific training that enables them to deal effectively with any such risk if applicable.

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 Information Asset Owner. These are still subject access requests but have specific conditions for e.g., 3rd Party requests.

Data transfers

All physical 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 actual transfer of personal data outside of the EEA is prohibited unless one or more of the physical data transfer safeguards, or exceptions, apply:

Information asset register/data inventory

ELA has established a data inventory as part of its approach to address risks, which determines:

- Business processes that use personal data.
- Source 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.
- Recipients, and potential recipients, of the personal data.
- The role of ELA throughout the data flow.
- Key systems and repositories.
- Any data transfers; and
- All retention and disposal requirements.

ELA 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 ELA, and in relation to processing undertaken by other organisations on behalf of ELA.

ELA shall manage any risks identified by the risk assessment of introducing new software/new processes in order to reduce the likelihood of a non-conformance with this policy and reduce the risk of a data breach/Non-compliance under GDPR.

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 persons, ELA shall, prior to the 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.

Where, as a result of a DPIA, it is clear that ELA is about to commence processing of personal data that could cause damage and/or distress with an increased risk of a data breach to the data subjects, the decision as to whether or not ELA may proceed must be escalated for review to ELA Risk Assurance Team through the Security Incident Management procedure.

Organisation of Information Security

1.21 Management of Information Security

Ultimate responsibility for information security rests with ELA Executive Committee.

At an operational level, responsibility for information security rests with the service line Managers.

The Data Compliance Manager could provide a quarterly report to the HEAD OF MIS, COMPLIANCE & ADMIN covering (as a minimum) the following items:

- An assessment of overall compliance with the information security policies and procedures.
- A plan for addressing any material non-compliance.
- Helping identify if there is a viable need for additional investment in order to ensure continued compliance with the information security policies and procedures.
- Any proposed amendments or additions to the information security policies and procedures.

1.22 Co-ordination with Additional Functions

The ELA Risk Assurance team will meet no less than 4 times per year and adhere to the Terms of Reference set out below.

1.22.1 Risk Assurance team's Terms of Reference (ToR)

- To take overall responsibility for Information Security Management and will include representation from:
  - Head of MIS, Compliance & Admin.
  - IAOs.
  - Human Resources.
- Define ownership and responsibility for Information Security Policy and Procedures.
- Review Information Security Policy within the organisation.
- Have representation on the Executive board meetings to address security issues.

1.23 Authorisation Process for Information Processing Systems

To ensure that information security is not undermined by the introduction of non-standard technology into ELAs IT infrastructure, all acquisitions of IT assets and services require the notification/approval of the Head of MIS, Compliance & Admin.

1.24 Restriction Agreements

Employees may be required to sign restriction agreements as part of their standard terms and conditions. Whenever there is a need to share ELAs restricted information with a third party, a suitable restriction (or non-disclosure) agreement will be executed with that third party prior to disclosure.

Restriction Agreements (or non-disclosure agreements) must be signed by a designated authorised signatory of ELA.

1.25 Contact with Authorities and Special Interest Group

ELA shall maintain appropriate contacts with relevant authorities and Special Interest Groups.

The Head of MIS, Compliance & Admin (& as part of the Executive Steering Group) will maintain regular contact with:

- Central Government Authorities to provide security advice as necessary.
- National Cyber Crime Unit
- Expert 3rd party suppliers

The ELA Risk Assurance team shall also draw advice from external security consultants and legal aids as necessary.

1.26 Independent Review and Advice

ELA will engage a suitably qualified independent third party to review, assess and advise on aspects of its information security regime on a regular basis.

As a minimum, the third party may undertake the activities referred to in this section annually or when there has been a significant change to the infrastructure.

The ELA Risk Assurance team will maintain records of all such reviews and assessments and will present the principal findings to the Executive Committee.

The ELA Risk Assurance team will review the choice of the external security partners annually.

The performance of the security partners will be governed by a formal contractual arrangement covering definitions of services to be provided, and all associated commercial terms.

The framework for the activities of the security partner is as follows:

Activities include:

- Advise and support the Risk Assurance team to develop and implement processes that identify and address evolving privacy/data protection risks inherent in ELA's operations.
- Leading on from the Risk Assurance, work with ELA's Senior Management & establish an organisation-wide privacy/data protection oversight committee.
- Assist in the identification, implementation, and maintenance of organisation privacy/data protection policies and procedures in coordination with all relevant stakeholders.
- Assist business functions with definition of function-level privacy/data protection processes and procedures.
- Initiate, facilitate, and promote activities to foster privacy/data protection awareness within ELA and all related entities.
- Support the development of a training strategy and materials and conduct company-wide training to ensure that employees are well-informed on key Information Security Policy elements.
- Assist in the definition and adoption of privacy impact assessment processes, including maturity assessments.
- Guide Employees and project management on conducting Privacy Impact Assessments including risk analysis and mitigation.
- Lead and coordinate investigations into privacy/data protection breaches and complaints and report findings to the Risk Assurance team.
- Undertake remedial action as requested (and if appropriate) by the Risk Assurance team. (Work may be considered outside of the scope of the Support contract and as such attract further investment requirement).

1.27 External Parties

Where a business requirement is identified for an external service provider or sub-contractor to be granted access to ELA's information processing systems (both electronic and paper based) an assessment will be made of the potential impact of that access on ELA's information security controls.

The third party will be required to commit to ensuring compliance with those aspects of ELA's information security policies and procedures that are relevant to the proposed engagement and this commitment will be recorded in a written agreement.

1.28 Customers/Suppliers/Employer/Learners and Security

Where a solution for a particular Client/Employer/Learner/Supplier potentially requires an extension of the ELA's infrastructure to be physically located at the premises of the Client/Supplier (or at other premises nominated by the Client/Supplier), the Client/Supplier will be required (as far as reasonably practical) to commit to ensuring compliance with those aspects of ELA's information security policies and procedures that are relevant to the proposed engagement and this commitment will be recorded in a written agreement.

Risk Appetite

1.29 Levels of Risk

By defining its information security risk appetite, ELA can derive an appropriate balance between innovation and caution. ELA can develop processes and polices based on the level of risk permitted and enforce consistency of approach across the firm.

Defined acceptable levels of risk also means that resources are not expended on further reducing risks that are already at an acceptable level.
Using a pre-defined 5-point scale the level of risk ELA is prepared to carry is perceived as a mixture of "Cautious" and "Open".

1. Averse - Avoidance of risk and uncertainty is a key organization objective.
2. Minimal - Preference for ultra-safe options that are low risk and only have a potential for limited reward.
3. Cautious - Preference for safe options that have a low degree of risk and may only have limited potential for reward.
4. Open - Willing to consider all potential options and choose the one most likely to result in successful delivery, while also providing an acceptable level of reward and value for money.

5. Hungry - Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk.

1.30 Measuring Risk

Precise measurement is risk is not always possible and risk appetite will sometimes be defined by a broad statement of approach.

Information Asset Definition

An Information Asset is:

1. A body of information that should it either became unavailable, corrupt, or was accessed by unauthorised persons or systems the business would cease to function/operate/realise its business outcomes for a period of time or cause contractual obligations to be severely impacted.
and/or

2. If ELA's competitors gained access, it would seriously undermine ELA's ability to retain a competitive advantage.
and/or

3. A compromise of confidentiality, integrity or availability would result in a fiscal penalty or reputational damage sufficiently severe to materially endanger ELA's financial targets.

Information Asset Ownership

Each identified information asset will have a nominated owner (Information Asset Owner) responsible for the following refer to Section 1.9):

Asset Management

1.31 Responsibility for Assets

All IT assets within ELA has a designated owner. The owner is responsible for ensuring that the asset is:

- Properly protected against theft or misuse.
- Only changed in accordance with ELA's Change Management Policy.
- Only accessed by authorised/approved persons.
- Connected to the Internet/cloud via an authorised and approved connection only.

1.32 Asset Register

The Head of IT Operations (3rd party service) _is responsible for ensuring the ELA's IT Asset Register is managed and maintained, including a 3rd party IT service provision, in accordance with the following procedures:

- Each IT Asset will have an Asset Number, Model Number and Location recorded against it in the IT Asset Register.
- The IT Asset Register shall specify the owner of each IT Asset. This will be updated as necessary when people leave the organisation or change role.
- The IT Asset Register shall specify whether the asset is covered by maintenance or support arrangements, and if so, who is the service provider and when does renewal occur.

The Head of IT Operations (3rd party service) will be responsible for notifying the Head of MIS, Compliance & Admin of any changes to the information relating to any asset for which they are responsible.

The Head of MIS, Compliance & Admin shall carry out spot checks of a random sample of the information held in the IT Asset Register on a six-monthly basis.

1.33 Maintenance and Support of IT Assets

All ELA's IT assets will be covered by current maintenance and support arrangements (other than "commodity items" such as keyboards, mice, and monitors).

Details of the maintenance and support provider will be included in the IT Asset Register together with information about the renewal date.

It is the responsibility of the Head of IT Operations (3rd party service provision) to ensure timely renewal.

1.34 Decommissioning IT Assets

An IT Asset shall only be decommissioned following explicit instruction, from the Head of MIS, Compliance & Admin / Head of IT Operations.

Following receipt of an instruction to decommission an IT Asset, the IT Department shall ensure that the impact of the decommissioning is fully understood by all relevant parties and that (where necessary) a replacement asset will be made available in a timely manner to ensure full continuity of services to users.

To ensure no inadvertent disclosure of data stored on the item that is to be decommissioned, decommissioning will be in accordance with the procedure in this section.

1.34.1 Procedure for decommissioning IT Assets

When a hardware asset is decommissioned, the IT Department shall ensure that all information stored on decommissioned hardware is irretrievably destroyed through low level formatting or physical destruction of the storage media. If this function is outsourced to a 3rd Party proof of destruction must be obtained through authenticated certificates of disposal.

Equipment will be decommissioned and disposed of in accordance with the Waste Electrical and Electronic Equipment recycling (WEEE) regulation.

Following completion of the decommissioning, the Head of MIS, Compliance & Admin / Head of IT Operations shall confirm that the decommissioning has been properly performed in the monthly Management report issued to the Executive Committee.

1.35 Data Encryption

All Protected and Restricted data processed within an Information Asset will be to FIPS-140/2 standard when at rest or being transmitted.

All information with a classification of Protected and Restricted will be encrypted when stored on any mobile device.

All information with a classification of Protected and Restricted will be encrypted when transmitted by e-mail.

1.36 Retention of Records

The required retention periods, by record type, are recorded in the data inventory under the following categories:

- Record type
- Retention period
- Retention period to start from (at creation, submission, payment, etc.)
- Retention justification
- Record medium
- Disposal method

Information Security Incident Management

1.37 Procedure for Reporting Logging of Security Incidents

All Incidents must be reported to the IT Service Desk (3rd party provision)

Example incidents include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data (e.g., Payslip) to an incorrect recipient
- computing devices containing personal data being lost or stolen.
- alteration of personal data without permission; and
- loss of availability of personal data. (e.g., A system is offline)

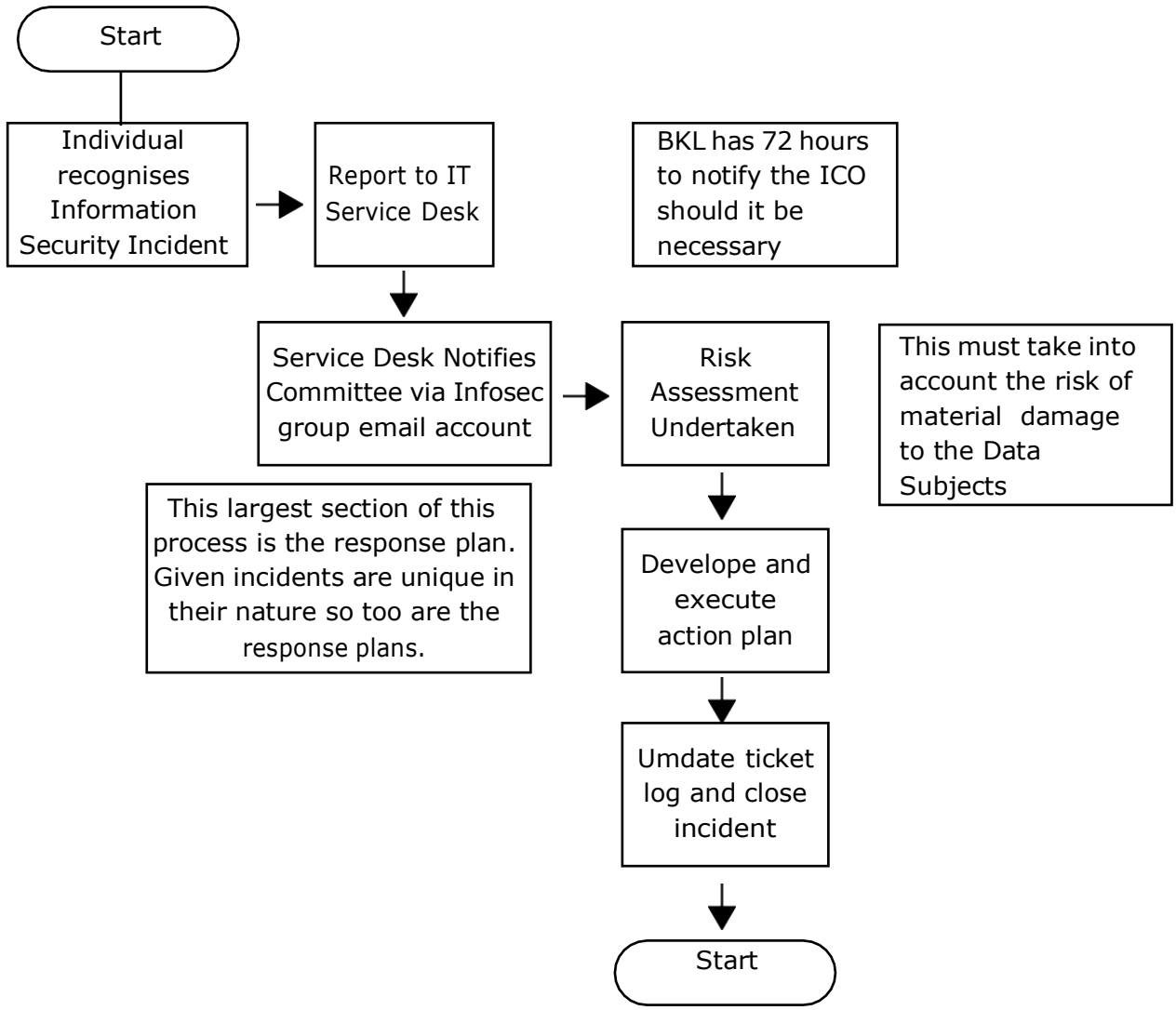
An Incident can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Cyber Crime
- Social engineering attacks where information is obtained by deceiving the organisation who holds it.

Immediately an Incident is discovered it should be reported to the IT Service Desk who will inform ELA Risk Assurance team nominee immediately. In the event that ELA Risk Assurance Team nominee is not available the Head of MIS, Compliance & Admin or appropriately approved stand-in will be notified.

ELA Risk Assurance team nominee will assess the risk ad if deemed necessary will convene an emergency Group Risk Assurance Team meeting (via Teams conference/video call) to raise the issue and activate the Information Security Incidents Response Process.

1.38 Information Security Incidents Response Process



1.39 Management of information security incidents

1.39.1 Responsibilities and procedures

1.39.1.1 Initial Risk Assessment

- Which classification of data is affected?
- Has a personal data breach occurred?
- Does the data breach involve data relating to living individuals?
- Is there likely to be a risk to the individual's right and freedoms?
- Has the data been contained and the risk to the data subjects mitigated?

Based on these questions it is possible to determine whether the breach may reach the threshold to report to the ICO and inform which relevant parties need informing.

1.39.1.2 Containment and recovery:

Initial actions will include:

- Establishing who needs to be made aware of the breach and where appropriate, inform the relevant parties (the Police, Data Subjects and ICO for example).
- Agreeing what actions need to take place in the action plan.

1.39.1.3 Record and Close:

- A written report of the incident will be produced and filed.

As a minimum, the report must detail:

- Circumstances leading up to the incident.
- The rationale for the decision taken as to whether or not to report to interested parties.
- A timeline of events during the first 72 hours.
- A copy of the action plan.

1.39.2 Notification of incidents

As part of managing a security breach ELA will inform people and organisations as appropriate:

- Individuals who may be affected by the breach.
- Funding / Contractual Bodies
- Regulatory Bodies
- Information Commissioner's Office within 72 hours (Article 33)
- Insurers
- Banks.

The notification will include a description of how and when the breach occurred and what data was involved. Additionally details of what ELA have already done to respond to the risks posed by the breach will be included.

ELA will also provide contact details should the above require further information.

1.39.3 Learning from information security incidents

The cause of the breach will be fully investigated. As such the following steps will be taken:

- Confirmation that data is lost or missing – this may take the form of a physical search.
- Interviews with Employees and any other relevant persons
- Written report on what has happened.
- Take action to recover data if possible.

Following any investigation into a security breach ELA will evaluate its effectiveness in dealing with it.

A review will of procedures will be undertaken to ensure that they remain fit for purpose.

1.39.4 Collection of evidence

ELA shall maintain a process to collect, retain and protect the chain of evidence relating to security incidents.

Business Continuity Management

1.40 Information security aspects of business continuity management

Please refer to the ELA Business Continuity Policy for further information.

Compliance

1.41 Compliance with legal requirements

ELA is committed to ensuring that it complies with all relevant legal, regulatory, and contractual obligations to which it is subject.

1.41.1 Prevention of misuse of information processing facilities

The following warning shall be implemented as part of the log-on process informing employees of their requirements under the Computer Misuse Act.

"This computer system is operated on behalf of ELA.

Only authorised users are entitled to connect and/or login to this computer system. If you are not sure whether you are authorised, please disconnect immediately and contact your line manager to request/confirm access."

1.41.2 Employee Training

All ELA employees will receive appropriate and proportional training in regard to understanding and complying with this policy.

1.42 Compliance with security policies and standards, and technical compliance

1.42.1 Compliance with security policies and standards

Employees shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

About this document

Content Owner: Farhan (Fuz) Zaidi, - Head of MIS, Compliance & Admin	**Owning Team:** Executive
For further information, please contact: Farhan (Fuz) Zaidi - Head of MIS, Compliance & Admin	

APPENDIX A – Subject Access Request Record

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					
Home					
Work					
Mobile					
Email address					
Date of birth					
Details of identification provided to confirm name of data subject:					
Details of data requested:					
Please explain briefly why you are requesting this information to be disclosed to the third party (if applicable)'					

1.44 Details of Person Requesting the Details (if not the Data Subject)

Are you acting on behalf of the data subject with their *[written]* or other legal authority?			Yes ☐ No ☐			
If 'Yes' please state your relationship with the data subject (e.g., parent, legal guardian, or solicitor)						
Please enclose proof that you are legally authorised to obtain this information.						
Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐	
Surname						
First name(s)						
Current address						
Telephone number:						
Home						
Work						
Mobile						
Email address						

1.45 Declaration

I, ……, the undersigned and the person identified in (1) above, hereby request that ELA provide me with the data about me identified above.

Signature: Date:

SAR form completed by (employee name):

I, ..., the undersigned and the person identified in (1.1) above, hereby request that ELA provide me with the data about the data subject identified in (1) above.

Signature: Date:

SAR form completed by (employee name):

This form must immediately be forwarded to ELA's Data Protection Manager / Information Asset Owner.

APPENDIX B- Definitions

The GDPR refers to a number of data protection terms such as pseudonymisation, minimisation and encryption.

These are discussed briefly in turn.

1.46 Pseudonymisation

Pseudonymising personal data can reduce the risks to data subjects and help controllers and processors meet their data protection obligations by ensuring that the additional information that attributes personal data to a specific data subject is kept separately.

The GDPR defined pseudonymisation as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

An example of pseudonymised data is as follows:

In Table 1 it is easy to identify each of the data subjects by Data Subject #, First Name & Last Name.

Tables 2 and 3 provide additional information about Data Subject 3 but because they are held separately and segregated from each other, it is not possible to identify the 'natural person'.

Table 1:

Data Subject #	First Name	Last Name
1	Fred	Jones
2	Albert	Einstein
3	Erin	Brockovich
4	John	Lewis

Table 2:

Data Subject #	Sex	Age
3	F	55

Table 3:

Data Subject #	Customer ID	Company Address 1	Company Address 2	Company Address 3	Company Post Code
3	101234	The Surgery	Somewhere St	Anyplace	Postcode 1

APPENDIX B- Definitions

1.47 Minimisation

The third principle of data protection specifies that personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

This obliges ELA to obtain and use only those pieces of information that are necessary for the data controller's purpose(s) for processing such information. Holding any additional personal data on individuals is unlawful.

1.48 Encryption

ELA has determined that mobile devices require encryption. As a matter of company policy, any device with personal data stored on it must use encryption to protect this data.

The Information Commissioner's approach to encryption of mobile devices is described, on their website – "By their very nature mobile devices such as laptops, smartphones and tablets have a high risk of loss

or theft. Encryption of the data contained on the device can provide an assurance that, if this happens, the risk of unauthorised or unlawful access is significantly minimised."

Non-mobile devices, such as desktop PCs and servers, have a lower risk of loss or theft when they are stored and used in a secure location, e.g., in a server room with restricted access. Although encryption is not generally used in non-mobile devices, ELA recognises that there is still a risk of loss or theft of a disk or the device itself (e.g., during a break-in). Therefore, using encryption on non-mobile devices is beneficial especially when the physical security cannot be maintained at an appropriate level. Therefore, non-mobile device encryption will be risk assessed annually.

1.49 Laptop whole-disk encryption

Sensitive information that is used on a laptop should be encrypted to the appropriate standard (currently considered FIPS140/2). Of course, any other confidential information – financial data, customer information, and so on – should also be encrypted to protect it if the laptop is ever lost or stolen.

The drawback with encryption solutions that only encrypt those files that contain confidential information is that laptop users don't always ensure they save data into these folders, and these encryption solutions do not automatically encrypt temporary files or caches. As a result, and in order to reduce exposure, ELA could use whole-disk encryption (also called full-disk encryption) that automatically encrypts all files stored on the laptop hard disk.