Data Protection Policy

Version Control	
Approved By	Gary Conduct
Version	GDPR07 Version 4.0: 31/03/2025
Policy became operational on:	November 2021
Next Review Date	March 2026

Context and Overview

Introduction

We hold personal data about our employees, associates, customers, suppliers, learners, and other individuals for a variety of business purposes. The aim of the Data Protection Policy is to ensure that as an organisation we comply with the requirements of UK General Data Protection Regulation and the UK Data Protection Act 2018. The GDPR places a duty on us as a business to protect the personal information held on our employees and clients

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. This policy requires staff to ensure that Brad Lawrence, Data Protection Lead be consulted before any significant new data processing activity is initiated to ensure that the relevant compliance steps are addressed.

Definitions

Term	Definition
Business Purposes	The purposes for which personal data may be used by us, including: ▪ Personnel ▪ Administrative ▪ Financial ▪ Regulatory ▪ Payroll ▪ Business Development ▪ Delivering Training *Business purposes include the following:* ▪ Compliance with our legal, regulatory, and corporate governance obligations and good practice ▪ Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests ▪ Ensuring business policies are adhered to (such as policies covering email and internet use) ▪ Operational reasons, such as recording transactions, training, and quality control, ensuring the confidentiality of commercially sensitive information and client information, credit scoring and checking ▪ Investigating complaints ▪ Checking references, ensuring safe working practices, monitoring, and managing staff access to systems and facilities and staff absences, administration and assessments ▪ Monitoring staff conduct, disciplinary matters ▪ Marketing our business

	▪ Improving services
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, 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. *Personal data we gather may include information about individuals':* ▪ contact details ▪ educational background ▪ financial and pay details ▪ qualifications, education, and skills ▪ marital status ▪ nationality ▪ job title, and CV.
Special Categories of Personal Data	Special categories of data include information about an individual's: ▪ racial or ethnic origin ▪ political opinions ▪ religious or similar beliefs ▪ trade union membership (or non-membership) ▪ physical or mental health or condition ▪ genetic and biometric information ▪ Criminal convictions, and related proceedings, are treated in the same way as special categories without Any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data Controller	The legal person or entity, organisation, 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. Explosive Learning Solutions is a data controller.
Data Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Data Controller. Data processors who process data on behalf of Explosive Learning Solutions include: ▪ King Loose & Co Accountants: to review and assess our financial conduct ▪ Pension Advisors, providing advice and guidance on employee pensions. ▪ Wavenet (external IT Support) ▪ Breathe HR

	▪ Accessplanit CRM ▪ SpecSavers: provide access to free eye-tests.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether 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.
Supervisory Authority	The national body responsible for data protection. The supervisory authority for Explosive Learning Solutions is the Information Commissioners Office (ICO).

Why this policy exists

This data protection policy ensures that Explosive Learning Solutions:

- Complies with data protection law and follows best practice
- Protects the rights of staff, clients, and suppliers
- Is transparent about how it stores and processes individual's data
- Protects itself from the risks of a data breach.

This policy supplements our other policies around acceptable use of internet and email, and the measurement of IT and security. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

This policy should be read in conjunction with the Handling Subject Access Requests and Handling Data Breaches policies.

The Principles of Data Protection

Data protection is about protecting people from misuse of their personal information. Explosive Learning Solutions regards the lawful and correct treatment of personal information as very important to successfully achieving the aims of the business, and to maintaining stakeholder trust and confidence.

These rules apply regardless of whether data is stored electronically or on paper. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The GDPR requires that data:

- Is processed fairly, lawfully and in a transparent manner;
- Is collected and processed only for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes;
- Is adequate, relevant and limited to what is necessary for those purposes;
- Is accurate, up to date and not kept in an identifiable form for longer than necessary for the purposes for which it is processed.
- Is processed in accordance with the data rights of individuals
- Is securely held, including protection by technical and organizational measures, against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The GDPR also gives individuals the right to access, delete, correct or receive in an easily transferable format, where applicable, personal information held by the business upon request.

Accountability and Transparency

The GDPR requires that organisations demonstrate compliance with the regulation and are accountable for their use of personal data. Organisations must also be transparent with individuals about how they will use the personal data they are responsible for. We will demonstrate compliance through documented plans, policies and procedures as well as maintaining an up-to-date log of our processing activities (the Register of Processing Activities). We will be transparent with individuals through the appropriate use of privacy information notices.

People, Risks and Responsibilities

Policy Scope

The policy applies equally to full time and part time employees on a substantive or fixed term contract and to associated persons who work for Explosive Learning Solutions**,** such as agency staff, investors, contractors, others employed under a contract of service. It stipulates their duties and responsibilities for the effective handling of personal and sensitive data, to comply with the policy and legislative, financial, and best practice requirements.

The policy applies to all personal and sensitive data collected, handled, and stored by Explosive Learning Solutions, in electronic and paper formats. This can include:

- Job Applications and CVs
- Educational background and qualifications

- Financial and Payroll information
- Employee details (including marital status, nationality, next of kin)
- Health information for staff (e.g., sick record)
- Client accounts (including signatures on contracts, financial transactions)
- Associate details (including security clearance, skills tree, CV.)
- Learner/Student information, including learning difficulties, contact details, dietary requirement, exam results, renewal dates etc.,
- Examination Institutions, including information to be shared, contact details.

Data Protection Risks

This policy helps to protect Explosive Learning Solutions from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how the organisation uses data relating to them.
- **Reputational damage.** For instance, the organisation could suffer if hackers successfully gained access to sensitive data.
- **Financial damage.** For instance, if a significant personal data breach were to occur the ICO may impose a substantial financial penalty on the organization.

Data Controller

The GDPR determines the role of a Data Controller as a ‘legal’ person or company that determines the purposes and means of any personal information and is fully responsible for the actions of anyone processing data on behalf of the organisation. Explosive Learning Solutions is the Data Controller.

Responsibilities

Everyone who works for or with Explosive Learning Solutions must process personal data fairly and lawfully in accordance with individuals’ rights.

Each member of staff that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibilities:

- The Board of Directors is ultimately responsible for ensuring that Explosive Learning Solutions meets its legal obligations.

- **Brad Lawrence** will fulfil the role of **Data Protection Lead**. The **Data Protection Lead,** is responsible for:
    - Keeping the board updated about data protection responsibilities, risks, and issues.

- Reviewing all data protection procedures and related policies, in line with an agreed schedule.

- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals such as clients and employees to see the data Explosive Learning Solutions holds about them (also called Subject Access Requests).
- Checking and approving any contracts or agreements with third parties that may handle the organisation's sensitive data.
- Leading on responding to and managing a data protection breach
- Liaising with the ICO to report and investigate personal data breaches if required.

• **Wavenet** will fulfil the role of **IT Manager.** The IT Manager, is responsible for:

- Ensuring all internal systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work (please refer to Register of Processing Activities for each site)**.**

- Data should not be shared informally. When access to confidential information is required, employees can request it from their line manager.

- Explosive Learning Solutions will provide training to all employees to help them understand their responsibilities when handling personal data.

- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- Strong passwords must be used, and they must never be shared. They must not be stored centrally.

- Personal data must not be disclosed to unauthorised people, either within the organisation or externally.

- Data must be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of (please refer to Retention and Disposal Policy).

- Employees must request help from the Data Protection Lead if they are unsure about any aspect of data protection.

Our Procedures

Fair and lawful processing

Explosive Learning Solutions must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. If we cannot apply a lawful basis as outlined below, our processing does not conform to the first principle and will be unlawful. Individuals have the right to have any data unlawfully processed erased. We will ensure that any new processing activities are assessed with a privacy by design approach prior to undertaking the processing. The following procedure will ensure that we meet this requirement of the regulation.

Lawful basis for processing data

Explosive Learning Solutions must establish a lawful basis for processing data. Employees must ensure that any data they are responsible for managing has a documented lawful basis approved by the Data Protection Lead in the Register of Processing Activities. It is each employee's responsibility to check the lawful basis for any data they are working with and ensure all their actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent:** We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. **Contract:** The processing is necessary to fulfil or prepare a contract for the individual.

3. **Legal obligation:** We have a legal obligation to process the data (excluding a contract).

4. **Vital interests:** Processing the data is necessary to protect a person's life or in a medical situation.

5. **Public function:** Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. **Legitimate interest:** The processing is necessary for our legitimate interests and does not outweigh the individual's rights.

Deciding which condition to rely on

When Explosive Learning Solutions are assessing the lawful basis, we will first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. We cannot rely on a lawful basis if we can reasonably achieve the same purpose by some other means.

Where more than one lawful basis applies, Explosive Learning Solutions will rely on what will best fit the purpose, not what is easiest.

We will always consider the following factors and document the answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Explosive Learning Solutions commitment to accountability and transparency requires that we document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This will be achieved via a privacy information notice. This applies whether we have collected the data directly from the individual, or from another source.

Employees who are responsible for assessing the lawful basis and implementing the privacy notice for new processing activities must have them approved by the **Data Protection Lead**.

Data Storage

These rules describe how and where data will be safely stored. Questions about storing data safely can be directed to either the Data Protection Lead or IT Manager.

When data is stored on paper, it will be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files must be kept in a locked drawer or filing cabinet**.** The keys must be kept separately and securely.

- Employees must make sure paper and printouts are not left where unauthorised people could see them**,** like on a printer.

- Data printouts must be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Personal data must be protected by strong passwords that are changed regularly and never shared between employees.

- If personal data is stored on removable media (like a USB drive or external hard drive), these must be encrypted at all times and kept locked away securely when not being used.

- Personal Data must only be stored on our designated drives and servers. Personal data must not be uploaded to unapproved external cloud computing services, like Dropbox for example.

- The ELS SharePoint site containing personal data is a secure location and is maintained by Wavenet.

- Personal data will be backed up frequently. These backups will be tested regularly, in line with our standard back procedures as documented in our IT Policy

- Personal data must never be stored directly to laptops or other mobile devices like tablets or smart phones if they are not adequately protected with passcodes (mobile devices) and / or encryption (laptops).

- Where personal data is stored on laptops or tablets for ease of access while working remotely, regular reviews must be undertaken to ensure the accuracy of the documents on the server and copies stored on other devices are securely destroyed once they are no longer needed for remote access purposes.

- All servers and computers containing data will be protected by approved security software and a firewall.

Data Use

Personal data is of no value to Explosive Learning Solutions unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft:

- When working with personal data, employees must ensure the screens of their computers are always locked when left unattended.

- Personal data must not be shared informally. Careful consideration must be taken before sharing personal data via email, as this form of communication is not secure. Additional checks to verify that the email is only being sent to individuals who have permission to see the data must be in place.

- Special Categories of Personal Data must be encrypted before being transferred electronically. The Data Protection Lead can explain how to send data to authorised external contacts.

- Personal data must never be transferred outside of the United Kingdom (UK).

- Employees must not save copies of personal data to their own computers. Always access and update the central copy of the data.

- Employees must not work on confidential or personal data in public areas (e.g., cafes or public transport) where there is a high risk of information being seen by other people nearby. If mobile working is necessary, the Data Protection Lead can provide additional security measures to protect the information so it cannot be seen (e.g., screen protectors for laptops or tablets).

- Employees must consider their location when talking on the phone or meeting with clients when discussing personal or confidential details. The reception area, public places and public transport are not suitable locations to hold confidential conversations.

Data Retention and Disposal

Explosive Learning Solutions will ensure that data will be stored for only if it is needed or in line with required statute and will be disposed of appropriately.

- This is supported by its Data Retention and Disposal Policy, which outline the organisation's requirements under this section of the policy.

- Explosive Learning Solutions will log all data assets on the Register of Processing Activities, which will be reviewed and updated every six months to monitor compliance with the Retention and Disposal policy.

- It is the IT Manager's responsibility to ensure all personal and organisation data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

- Maintaining Records of Processing Activities (ROPA) in compliance with the Data Protection Legislation

- Explosive Learning Solutions will make it easy for data subjects to update the information the organisation holds about them. This is possible by calling the organisation on: 01235 861805 or emailing us on info@explosivelearningsolutions.com.

- Data must be updated as inaccuracies are discovered. For instance, if a customer or associate can no longer be reached on their stored telephone number, it will be removed from the relevant database, and we will try to establish what the correct details are.

Data Accuracy and Relevance

Explosive Learning Solutions will ensure that any personal data that is processed is accurate, adequate, and relevant and not excessive, given the purpose for which it is obtained. Explosive Learning Solutions will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

It is the responsibility of all employees who work with personal and or personal sensitive data to take reasonable steps to ensure it is kept accurate and up to data as possible.

- Data will be held in as few places as necessary. Staff must not create any unnecessary additional data sets. [Please see Register of Processing Activities for the complete list of information assets and where they are stored].

- Staff will take every opportunity to ensure that data is updated. For instance, by confirming a client's details when they call.

- If an individual identifies that personal data held by Explosive Learning Solutions is inaccurate and requests that the organisation updates the information, the organisation will review the data and make the appropriate updates without undue delay and within 30 days.

- Staff must take reasonable steps to ensure that personal data that Explosive Learning Solutions holds on them is accurate and updated as required, for example if their personal circumstances change or they change address.

Transferring Data Internationally

There are restrictions on international transfers of personal data. Explosive Learning Solutions does not permit the transfer of personal data anywhere outside the United Kingdom (UK) without first consulting the Data Protection Lead.

Data Audit and Register

ELS has a risk governance framework in place and undertakes risk assessment at regular intervals to regulate and manage risks associated with the processing of personal data (staff, delegates etc.)

Where required ELS undertakes Data Protection Impact Assessments regular data audits to manage and mitigate risks will inform the Register of Processing Activities. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. It will be reviewed on a regular basis and at a minimum every 12 months, or when the organisation undertakes new data processing.

Individuals' Rights

Explosive Learning Solutions will ensure any use of personal data is justified using at least one of the conditions (e.g., consent, legitimate interest, performance of a contract, legal obligation) for processing and this will be specifically documented within the Register of Processing Activities. All staff that are responsible for processing personal data will be aware of the conditions for processing. The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Subject Access Requests

All individuals who are the subject of personal data held by Explosive Learning Solutions are entitled to:

- Ask **what information** the organisation holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the organisation is **meeting its data protection obligations**.

If an individual contacts the organisation requesting this information, this is called a subject access request.

Subject access requests from individuals can be made by email, addressed to the Data Protection Lead at mailto:babs@clarkerowesolicitors.co.ukinfo@explosivelearningsolutions.com or in writing to: Data Protection Lead, Explosive Learning Solutions Ltd, 4 The Terraces, Library Avenue, Harwell Science and Innovation Campus, Didcot, Oxfordshire, OX11 0SG. Explosive Learning Solutions may supply a standard request form, although individuals do not have to use this. If a subject access request is sent directly to another Explosive Learning Solutions employee, they must pass it immediately to the Data Protection Lead to handle.

The Data Protection Lead will always verify the identity of anyone making a subject access request before handing over any information. One of the following forms of ID will be required:

- Passport
- Photocard Driving Licence

Explosive Learning Solutions will aim to provide the relevant data without delay, and certainly within 30 days. Where the request is more complex, we will notify the individual making the request of any likely delay and extension period required. For more information, please refer to the Handling Subject Access Requests Policy.

Data Portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. The right to portability only applies:

- to personal data that the individual has provided to Explosive Learning Solutions
- where the processing of personal data is based on the individual's consent or for the performance of a contract
- when processing is carried out by automated means (i.e., electronically)

Requests from individuals can be made made by email, addressed to the Data Protection Lead at mailto:babs@clarkerowesolicitors.co.ukinfo@explosivelearningsolutions.com or in writing to: Data Protection Lead, Explosive Learning Solutions Ltd, 4 The Terraces, Library Avenue, Harwell Science and Innovation Campus, Didcot, Oxfordshire, OX11 0SG.

The Data Protection Lead will always verify the identity of anyone making a request under the right to portability their personal data before handing over any information. One of the following forms of ID will be required:

- Passport
- Photocard Driving Licence

These requests should be processed within one month, provided there is no undue burden, and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free. The data will be provided to the individual in a structured, commonly used, and machine-readable format, e.g., a csv file, and will be transferred to them securely.

Right to Erasure

In certain circumstances, an individual may request that any information held on them by Explosive Learning Solutions is deleted or removed, and any third parties who process or use that data must also comply with the request.

An individual has the right to have their information erased if:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for
- the legal basis on which the organisation is holding the personal data is consent, and the individual withdraws their consent
- the legal basis on which the organisation is processing the data is legitimate interests, and the individual objects to the processing of that data, and the organisation is unable to demonstrate that overriding legitimate interests to continue this processing exists
- the organisation has processed the personal data unlawfully
- the organisation must delete the data to comply with a legal obligation

An individual does not have the right to have their information erased if the processing of their personal data by Explosive Learning Solutions is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation
- for the performance of a task carried out in the public interest or in the exercise of official authority
- for the establishment, exercise, or defence of legal claims

Requests from individuals can be made by email, addressed to the Data Protection Lead at info@explosivelearningsolutions.com or in writing to: Data Protection Lead, Explosive Learning Solutions Ltd, 4 The Terraces, Library Avenue, Harwell Science and Innovation Campus, Didcot, Oxfordshire, OX11 0SG. They may also make the request verbally in person or via telephone: 01235 861805.

Explosive Learning Solutions will aim to provide the relevant data without delay, and certainly within 30 days. Where the request is more complex, the Data Protection Lead will notify the individual making the request of any likely delay and extension period required.

If any personal data that is to be erased in response to an individual's request has been disclosed to third parties, the Data Protection Lead will inform those parties of the erasure (unless it is impossible or would require disproportionate effort to do so).

Data Breaches

Any data breach of personal information must be recorded by Explosive Learning Solutions**.** The GDPR sets out the requirements to respond to a personal data breach.

- Data controllers (Explosive Learning Solutions) must report certain types of data breach to the supervisory authority (Information Commissioners Officer (ICO)) without undue delay and within 72 hours or becoming aware of data breach.

- Data controllers will be required to notify individuals affected by the data breach in circumstances where it is likely to cause a high risk to their rights and freedoms.

- A breach notification to the ICO should include:
  - The nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned; and
    - Categories and approximate number of personal data records concerned.

  - The name and contact details of the Data Protection Lead.

  - A description of the likely consequences of the personal data breach.

  - A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measure taken to mitigate any possible adverse effects.

In order to effectively monitor data breaches, the Data Protection Lead will document each data breach in the Explosive Learning Solutions Data Breach Log file, including facts of the breach, the effects and action taken. The Data Protection Lead, with relevant support from staff in the organization, will assess the likely risk and impact on individuals affected by the breach immediately, and where necessary report to the ICO within 72 hours via the ICO website. Further details about the breach will be established using the data breach process.

ELS is registered with the UK Information Commissioner's Office (ICO), our registration number is **Z10607005.**

Data Breach Process

To understand why a breach occurred and prevent further breaches, the Data Protection Lead will:

- Determine how the breach happened.
- Determine what, if anything, could have been done to prevent it.
- Understand what can be done to prevent future breaches.
- Determine how soon the changes can be implemented
- Update and cascade training for employees as soon as possible
- Provide an update to individuals affected by the breach on the outcome of the investigation and what we are doing to prevent future breaches
- Provide an update to the Partnership Board on the outcome of the investigation and what we are doing to prevent future breaches
- Deal with any complaints
- Respond to any requests for further information from the Information Commissioner's Office (*if relevant*).

- implement and comply with recommendations from the Information Commissioner's Officer.

For full details of our Data Breach Process, including an incident report form, please read the Data Breach Policy.

Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act 2018 allows personal data to be disclosed to law enforcement agencies without consent of the data subject.

Under these circumstances, Explosive Learning Solutions will disclose requested data. However, the Data Protection Lead will ensure the request is legitimate, seeking assistance from the board and from the organisation's legal advisers where necessary.

Providing Information (Privacy Notices)

Being transparent and providing accessible information to individuals about how Explosive Learning Solutions will use their personal data is important to the organisation. To these ends, Explosive Learning Solutions has a privacy policy, setting out how data relating to individuals is used by the organisation. A version of this privacy statement is also available on the organisation's website: Privacy Notice Policy - ELS (elsbusinesstraining.co.uk)

The organisation will also include appropriate privacy information notices at the point where personal data is collected from individuals, for example at the point of recruitment.

Policy Compliance

If any user is found to have breached this policy, they may be subject to Explosive Learning Solutions disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Any unauthorised disclosure of personal data to a third party by an employee will be viewed seriously and may result in disciplinary proceedings.

The Board of Directors are accountable for compliance of this policy. A director could be personally liable for any penalty arising from a breach that they have made.

Review and revision

This policy must be reviewed every 12 months and, if appropriate, will be amended to maintain its relevance. Further reviews will be undertaken to reflect changes in legislation or standards. The Data Protection Lead will undertake policy review.