Version Control
Version: 6.0
Summary of Updates: British English compliance, QA improvements, designated person relocated to approval section, updated review dates.

Approval
Approved by: Neville Algar, Head of Education
T: 03 003 030 890
M: 07 880 198 243
E: n.algar@ignitesportuk.com
Updated Review Date: 2025-11-24
Next Annual Review: 2026

GDPR Policy

Contents

Version Control

Approval

Policy Statement

Scope

Data Protection Law

Data Protection Risks

Responsibilities

Guidelines for Staff

Data Storage

Data Use

Subject Access Requests

Disclosing Data

Monitoring and Review

Associated Policies

Version Control

Title			Version
GDPR Policy			1.0
Approval Body		**Date**	**Review Date**
Corporation		11/11/2024	11/11/2025
Policy Owner	Neville Algar		

Approval

Name	Neville Algar
Signature	*N.Algar*
Position	Head of Education

Policy Statement

Ignite Training needs to gather and use certain information about individuals. These can include employers, learners, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

This data protection policy ensures the company complies with data protection law and follows good practice. We endeavour to protects the rights of staff, customers and partners and are open about how we store and process individuals' data and protects ourselves from the risks of a data breach.

Scope

This policy applies to:

The head office and all branches of the company, all staff contractors, suppliers and volunteers working on behalf of the company and all learners and clients involved with the company.

It applies to all data that the company holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

Data protection law

The Data Protection Act 1998 and subsequently the General Data Protection Regulation May 2018; describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Data protection risks

This policy is to protect the company 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 company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with the company has responsibility for ensuring data is collected, stored and handled appropriately. Each team 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 responsibility:

The Data protection officer

- 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 subject access requests from individuals
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

The data protection officer is:

Name	Email	Telephone
Justin Merritt	J.Merritt@ignitesportuk.com	

The directors;

- Ensuring all 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.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters, learner applications.
- Addressing any data protection queries
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

Guidelines for Staff

The only people able to access data covered by this policy should be those who need it for their work.

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

The company will provide training to all employees to help them understand their responsibilities when handling data.

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

- Strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should 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.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data protection officer.

When data is stored on paper, it will be kept in a secure place where unauthorised people cannot see it, this includes locked filing cabinets in head office.

All staff should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

Data printouts should 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:

Data should be protected by strong passwords that are changed regularly and never shared between employees.

If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.

Servers containing personal data should be sited in a secure location, away from general office space.

Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

Data should never be saved directly to laptops or other mobile devices like tablets or smart phones. All servers and computers containing data should be protected by approved security software and a firewall.

Data use

When working with personal data, employees should ensure the screens of their computers are always locked when left unattended. Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure. Data must be encrypted before being transferred electronically. Personal data should never be transferred outside of the European Economic Area.

Data accuracy

The company is required by law to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible. Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets. Staff should take every opportunity to ensure data is updated. For instance, by confirming learners details when they call. Data should be updated as inaccuracies are discovered. For instance, if a learner can no longer be reached on their stored telephone number, it should be removed from the database. It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject access requests

All individuals who are the subject of personal data held by the company are entitled to:

- Ask what information the company 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 company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data protection officer named above. The data protection officer will aim to provide the relevant data within 14 days. The data protection officer will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, the company will disclose requested data. However, the data protection officer will ensure the request is legitimate, seeking assistance from the directors and from the company's legal advisers where necessary.

Monitoring and Review

The SMT will monitor the effectiveness and review the implementation of this policy with regards to its suitability, adequacy and effectiveness. Any improvements identified will be made as soon as possible. Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective. Employees and stakeholders are responsible for the success of this policy and should ensure they use it to disclose any suspected danger or wrongdoing. Employees and stakeholders are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries should be addressed to the SMT. This policy will be reviewed annually as a minimum and may be amended at any time.

Associated Policies

- Privacy Policy