SCALING UP
COACHES

Data Protection Policy

Policy Approved

To be reviewed annually

Review Date: April 2024

Signed: **Date:**

18/04/2023
18/04/2024
18/04/2025
18/04/2026

Scaling up Coaches
Lyndor
Hole-in-the-Wall
Ross-on-Wye
Herefordshire HR9 7JW

Data Protection Policy – Key Elements

What is the UK GDPR?

This is a European Directive that will be brought into UK law with an updated Data Protection Act for May 2018. Brexit will not change it.

The current Data Protection Act 1998 will be repealed and replaced with the Data Protection Act 2018.

What is the point of the UK GDPR?

The UK GDPR and new DPA exist to look after individual's data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

The UK GDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, We want to make sure information that we hold is kept secure and within the law.

What is Data?

Any information that relates to a living person that identified them. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

What are the key principles of UK GDPR?

Lawfulness, transparency and fairness.

Scaling Up Coaches must have a legitimate reason to hold the data, we explain this in the Data Privacy Notices on the website. We often ask for consent to use data for a particular purpose. If you wish to withdraw consent we have a form to complete to allow us to process your request. There are sometimes when you cannot withdraw consent as explained in 'Data Subjects Rights'.

Collect data for a specific purpose and use it for that purpose

So, data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. We do this when clients join Scaling Up Coaches and check on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event a dispute resolution process and complaint process can be accessed, using the suitable forms.

Retention

Scaling Up Coaches has a retention policy that explains how long we store records for. This is available on request.

Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information.

To support UK GDPR, Scaling Up Coaches will:

- make sure that all employees, including contract staff acting on Scaling Up Coaches' behalf, understand their responsibilities about information security under the 1998 Act.
- make sure they receive appropriate mandatory training, instruction and supervision so they can perform these duties effectively and consistently
- make sure they only have access to personal information that is necessary to their duties
- make sure that all others acting on behalf of Scaling Up Coaches are only given access to personal information that is necessary to the duties they perform and no more.
- handle any requests for access to personal data courteously, promptly and appropriately, making sure that either the data subject or their authorised representative have the proper right to access under the 1998 Act
- make sure that information provided is clear and explicit
- Manage reported security breaches appropriately and in line with the security breach management framework issued by the Information Commissioner's Office

Who is a 'data subject'?

Someone whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out a collection of details such as health conditions and ethnicity, which are more sensitive than names and phone numbers.

Data subjects' rights

Individuals have a right:-

- to be informed
- of access to data stored about them

- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for Scaling Up Coaches to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision-making and data portability that are not directly relevant in the business.

Who is a 'data controller'?

Scaling Up Coaches isn't required to have a data controller, however Wendy Lewis has been tasked with taking the main responsibility in controlling data that is associated with Scaling Up Coaches.

Who is a 'data processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the Local Authority.

Data controllers must make sure that data processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Not all businesses need a data controller if for example you aren't a public authority or carry out certain types of data processing especially that which isn't deemed high security. Schools, Hospitals etc. will need a DPO. Scale Up Coaches has assessed the guidelines and are exempt from needing a DPO (we will however have the highest standards and continue to maintain these for years to come).

Processing data

Scale Up Coaches must have a reason to process the data about an individual. Our privacy notices set out how we use data. The UK GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach we follow the procedure and take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data are:-

- consent obtained from the data subject
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.
- In addition, any special categories of personal data are processed on the grounds of explicit consent from the data subject
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of Luv4 Marketing
- existing personal data that has been made public by the data subject and is no longer confidential bringing or defending legal claims
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the Scale Up Coaches system.

Data Sharing

Data sharing is done within the limits set by the UK GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in Scaling Up Coaches systems.

Data Portability

The UK GDPR requires an organisation that stores data to enable transfer of that data from one organisation to another.

Employee data will be shared if required to enable new starters and leavers to take up new roles as easily as possible.

Breaches & Non Compliance

If there is non-compliance with the policy or processes, or there is a DPA breach as described within the UK GDPR and DPA 2018 then the guidance set out in the Breach & Non Compliance Procedure and Process needs to be followed.

Protecting data and maintaining data subjects rights is the purpose of this policy and associated procedures.

It is important that any non-compliance is brought to the attention of the Data Protection Officer to enable an action plan to be developed and implemented. This record will also serve as a useful mechanism to identify trends, risks and potential breach hazards.

By having an agreed timescale for review, identifying training needs that may be applicable to an individual or group of people will assist future compliance. See Appendix 1 for procedure.

Consent

Scaling Up Coaches will seek consent from staff, clients, licensees and franchisees to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the UK GDPR as “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 him or her”.

See Appendix 2 for further detail.

Consent and Renewal

On the Scaling Up Coaches website we have ‘Privacy Notices’ that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent Scaling Up Coaches will consider each situation on the merits and within the principles of UK GDPR.

Please complete the appropriate form.

Subject Access Request

As an organisation we collect and process data about individuals. We explain what information we collect, and why in our Privacy Notices.

Any individual, or person with parental responsibility, or young person with sufficient capacity to make a request is entitled to ask what information is held. Copies of the information shall also be made available on request. A form to complete is available.

To ensure that requests are dealt with in an effective and timely manner we may seek to clarify the terms of a request.

To collate and manage requests we have designated Wendy Lewis to coordinate all requests. Please ensure that requests are made on the form to Wendy Lewis.

Evidence of their identity, on the basis of the information set out and the signature on the identity must be cross checked to that on the application form. Discretion about employees and persons known to the Scaling Up Coaches may be applicable but if ID evidence is not required an explanation must be provided by staff and signed and dated accordingly

Exemptions to a SAR exist and may include

- Education, Health, Social Work records
- Examination marks and scripts
- Legal advice and proceedings
- National security, Crime and taxation
- Journalism, literature and art
- Research history, and statistics
- Confidential references

All data subjects have the right to know:-

- What information is held?

- Who holds it?
- Why is it held?
- What are the retention periods?
- That each data subject has rights. Consent can be withdrawn at any time (to some things).
- A right to request rectification, erasure or to limit or stop processing
- A right to complain

Many of these questions will be within the Privacy Notices on the website.

The information will be provided in an electronic format, usually within one calendar month of the request. However in some circumstances, for example Scaling Up Coaches is closed for holidays, this may be extended by up to another calendar month.

Physical Security

At Scaling Up Coaches , every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

All Staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party, are subject to contractual conditions to ensure GDRP and DPA compliance.

Hardware, copy files, hard drives and portable/removed storage will be destroyed accordingly using a company who are UK GDPR compliant. Due to the limited amount of times that this takes place a contract is not in place but will be sought should this be required.

Complaints & the Information Commissioner Office (ICO)

The Scaling Up Coaches Complaint Policy deals with complaints about Data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

All Staff must be aware of the complaints process. All complaints should be directed to the Data Protection Officer. If any member of staff is aware that a person wishes to complain they should direct the person to the Scaling Up Coaches website and complaints policy and form.

Data Protection Officer is responsible for dealing with all complaints in line with this procedure.

The Scaling Up Coaches complaints policy sets out the complaints process. This will be the basis for dealing with Data Protection Complaints and appeals. A written outcome will be provided.

If Scaling Up Coaches does not comply with a Subject Access Request within 1 month (subject to any extension), or refuses all or part of the request, written reasons will be provided, setting out the principles for the refusal. The data subject(s) will be notified of the right to complain directly to the Information Commissioner, whose details will be in the response.

You can complain if you have asked us to erase, rectify, not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

Review

A review of the effectiveness of Uk GDPR compliance and processes will be conducted by the Data Protection Officer every 12/24 months.

This policy applies to all permanent and temporary employees and those acting on behalf of Scale Up Coaches.

Appendix 1 - Data Protection Breach & Non Compliance Procedure

All staff must be aware of what to do in the event of a DPA / UK GDPR breach.

The 'Data Breach Flowchart' outlines the process.

The 'Data Breach Form' must be completed and updated as the process progresses.

Most breaches, aside from cyber-criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Everyone needs to understand that if a breach occurs it must be

swiftly reported. Examples of breaches are:-

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or portable data device, unencrypted mobile phone, USB memory stick or similar
- Sending an email with personal data to the wrong person
- Dropping or leaving documents containing personal data in a public place
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offense under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to Scaling Up Coaches (and subsequently its records) is being subjected to a virus or malicious attack, which

results in unauthorised access to, loss, destruction or damage to personal data.

What to do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach to the Data Controller, Data Protection Compliance Manager and DPO as soon as possible, this is essential.

The breach notification form will be completed and the breach register updated.
If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a coordinated manner with support from the DPO.

The breach report will be within 72 hours of becoming aware of the breach.
It may not be possible to investigate the breach fully within the 72 hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

Procedure – Breach notification data controller to data subject

For every breach Scaling Up Coaches will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.
If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Data Controller with support from the Data Protection Compliance Manager and DPO. Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.

A post breach action plan will be put into place and reviewed.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of staff, which may be the Data Management Compliance Officer or Data Protection Officer, but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

Date	Evidence Description	Secure storage location & confirmed date	DPO

Appendix 2 - Consent

Scaling UP Coaches will seek consent from staff, clients, licensees & franchisees to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the Uk GDPR as “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 him or her”.

Consent and Renewal

On the website we have ‘Privacy Notices’ that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of UK GDPR.

Please complete the appropriate form.

SCALING UP

COACHES