UK GDPR/Data Protection Policy

Including Subject Access Requests and Breach of Data Procedures

Version	**1.7**		
Author	**Oliver Trailor, amended by Elaine Highwood**		
Approved by	**SLT**		
Document Creation Date	29.1.2021	**Review Due**	12.08.2026
Distribution to	**All**		

Version	Review date	Comments	Author	Approved by
1.1	22.11.2021	Amendment to ESF retention rates	Elaine Highwood	SMT
1.2	29.1.2022	Reviewed no amendments made	Elaine Highwood	SMT
1.3	30.5.2022	Promotion and sign-up introductory information added	Elaine Highwood	SMT
1.3.1	30.8.2022	Role of Data controller and Data Protection Officer added	Elaine Highwood	SMT
1.3.2	30.3.2023	Amendment to ESF retention rates	Elaine Highwood	SMT
1.4	30.08.2023	Reviewed – general update on wording throughout and PICS and Altitude information added	Sam Mihalceanu, Mel Fuller; Elaine Highwood	SMT
1.5	30.03.24	Reviewed – no amendments made	Zoe Henley	SMT
1.6	12.08.24	Amended to read UK GDPR	Zoe Henley	SLT
1.7	12.08.25	Reviewed – no amendments made	Zoe Henley	SLT

This policy is version 1 of an amalgamation of 2 previous policies and should be read in conjunction with Runway Training's Data Security Policy and Privacy Policy.

Authorising Officer: Oliver Trailor, Managing Director

Signature:  **Date:** 12.08.25

Data Protection

Promoted during the sign-up process, this policy will form part of the Induction Process for all learners and will be accessible through their learner handbook, forming part of their Induction. Internal Stakeholders can access the policy through the shared drive, and all stakeholders can access it through Runway Training's Website.

All staff will be informed of the policy at Induction, which will form part of Runway's Mandatory training. Additional training/updates will be given as and when needed.

This policy will be reviewed annually or sooner if legislation/organisational changes impact the content of this policy.

Introduction

Runway Training needs to keep certain information about its employees, students, and other users to allow us to monitor recruitment, attendance, performance, achievements and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised, and legal obligations to funding organisations and the government can be upheld.

To comply with the law, information must be collected and used fairly, stored safely and not unlawfully disclosed to anyone . To do this, Runway Training must comply with the Data Protection Principles set out in the GDPR and Data Protection Act 2018 and stated above.

Runway Training and all staff or others who process or use personal information must always follow these principles.

Runway Training will keep a register of staff authorised to access and process learner and staff data, and these staff members will be asked to sign a confidentiality statement.

Scope

Key Principles

a) Personal data should be processed fairly and lawfully.

b) Personal data shall be obtained only for one or more specific and lawful purposes and shall not be processed in any manner incompatible with those purposes.

c) Personal data shall be adequate, relevant, and not excessive concerning their processing purposes.

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

e) Personal data shall not be kept for longer than is necessary.

f) Personal data shall be processed as per the individual's rights under the Act.

Purposes of obtaining data

To fulfil individuals' contracts of employment, monitor sickness and performance, equal opportunity policies, and otherwise administer the Company's business, we will use and process personal information relating to you, including:

a) Employment history

b) Personal circumstances

c) Educational qualifications

d) Sickness records

e) Medical records

f) Accident reports

g) Attendance records

h) Convictions

i) Performance appraisals

j) Disciplinary records

k) Ethnic or racial origins

l) Salaries

m) Benefits

In most cases, staff have provided information. In others, the information has been provided by the line manager, other employees, external referees, or your doctor regarding medical records.

Personal data about staff is held confidentially and Runway Training will only disclose it to others where there is a need to do so, e.g., to give information about earnings to Her Majesty's Revenue & Customs.

No sensitive data, such as information about health, racial or ethnic origins, criminal convictions, trade union membership, political or religious belief, will be divulged to a third party without your permission unless we have a specific legal requirement to process such data.

Accuracy of data

Any personal data held must be accurate. Staff must inform the Company if they believe their personal data is inaccurate or untrue or if they are dissatisfied with the information.

Right to access information

Under the legislation, staff are entitled to access certain personal data. If staff require access, staff should contact their line manager. The request should be made in writing, specifying the information required.

Responsibilities

Partners: The Partners are responsible for the oversight and implementation of this policy. Any information held by Runway Training that appertains directly to the Partners/Sub-contractors and/or their business information, learners and/or staff is accessed by Runway Training staff via restricted access only.

Senior Managers: It will be the responsibility of the senior managers to ensure compliance with the policy and to communicate the policy to all staff.

All Staff: All staff are responsible for ensuring that any personal data which they hold is kept securely and personal information is not disclosed in any way and to any unauthorised third party.

All Students and Staff: Learners and staff are responsible for ensuring that all personal data provided to Runway Training is accurate and current.

Compliance: Failure to comply with the data protection policy and procedure could result in disciplinary action.

Review: This policy and related procedures will be reviewed and issued on at least an annual basis

Responsibilities of staff

All staff are responsible for:

- Checking that any information they provide to Runway Training concerning their employment is accurate and up to date.
- Informing Runway Training of any changes to information, which they have provided, i.e., change of address.
- Informing Runway Training of any errors or changes. Runway Training cannot be held responsible for any errors unless the staff member has informed us of them.

All staff must comply with the following guidelines:

- All staff will process data about individuals regularly when marking registers, writing reports or references, or as part of a pastoral or academic supervisory role. Runway Training will ensure, through registration procedures, that all individuals give their consent to this type of processing, and are notified of the categories of processing, as required by the GDPR and Data Protection Act 2018.
- The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:
    - General personal details such as name and address.
    - Details about class attendance, coursework marks and grades and associated comments.
    - Notes of personal supervision, including matters about behaviour and discipline.
- Information that has the potential to identify protected characteristics of learners i.e. an individual's age, gender, or gender reassignment, ethnicity, disability, religion and belief, sexual orientation, trade union membership, or race is sensitive and can only be collected and processed with consent.
- All staff must ensure they comply with the data protection principles set out in the staff handbook. Staff must ensure that records are:
    - Accurate
    - Up to date
    - Fair
    - Kept and disposed of safely and as per the policy.
- Authorised staff are responsible for keeping all personal data secure. Staff must ensure that personal data is:
    - Put away in lockable storage.
    - Not left on unattended desks or tables.
    - Unattended ICT equipment should not be accessible to other users.
    - ICT equipment used off-site must be password-protected.
    - The use of memory sticks are restricted. Data files on memory sticks or email attachments used off-site containing personal data must be password-protected, and memory sticks must also be encrypted.

Personal data: This is data, including expressions of opinion, which relates to a living individual who can be identified from the data alone or from that data along with other information which you are in possession of or come into the possession of. Common examples of personal data include:

- Name
- Date of birth

- Home addresses
- Home/mobile telephone numbers
- Personal or business email addresses
- Payment details
- Call recordings

The list below is a non-exhaustive list of documents that may require password protecting, should they be sent to via email:

Assessment Evidence: e.g. Reports, Witness Testimonies, Discussion Evidence and Reflective Diaries Assessor Tracking Documents Certificates CPD Records CVs Enrolment Forms IQA Tracking Documents	IQA Feedback Reports Learner Assessment Plans Learner Claim Forms Learner Feedback / Progress Reports Learner Registration Details Learner Sample Lists Minutes of Team and Standardisation Meetings Placement Logs

Paper records containing personal data must be shredded where appropriate.

Responsibilities of the Data Controller

If you are a controller, you are responsible for ensuring your processing – including any processing carried out by a processor on your behalf – complies with the UK GDPR. Your UK GDPR responsibilities include the following:

- **Compliance with the data protection principles**: you must comply with the data protection principles listed in Article 5 of the UK GDPR.
- **Individuals' rights**: you must ensure that individuals can exercise their rights regarding their personal data, including the rights of access, rectification, erasure, restriction, data portability, objection and those related to automated decision-making.
- **Security**: you must implement appropriate technical and organisational security measures to ensure the security of personal data.
- **Choosing an appropriate processor**: you can only use a processor that provides sufficient guarantees that they will implement appropriate technical and organisational measures to ensure their processing meets UK GDPR requirements. This means you are responsible for assessing that your processor is competent to process the personal data in line with the UK GDPR's requirements. This assessment should consider the nature of the processing and the risks to the data subjects.
- **Processor contracts**: you must enter a binding contract or other legal act with your processors, which must contain a number of compulsory provisions as specified in Article 28(3).
- **Notification of personal data breaches**: you are responsible for notifying personal data breaches to the ICO and, where necessary, other supervisory authorities in the EU, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. You are also responsible for notifying affected individuals (if the breach is likely to result in a high risk to their rights and freedoms).

- **Accountability obligations**: you must comply with the UK GDPR accountability obligations, such as maintaining records, carrying out data protection impact assessments and appointing a data protection officer.
- **International transfers**: you must comply with the UK GDPR's restrictions on transfers of personal data outside of the UK.
- **Co-operation with supervisory authorities**: you must cooperate with supervisory authorities (such as the ICO) and help them perform their duties.

  Data protection fee: you must pay the ICO a data protection fee unless you are exempt.

Responsibilities of the Data Processing Officer

If you are a DPO, you are responsible for the following:

- inform and advise your employees about your obligations to comply with the UK GDPR and other data protection laws.
- monitor compliance with the UK GDPR and other data protection laws and with your data protection policies including managing internal data protection activities, raising awareness of data protection issues, training staff and conducting internal audits.
- advise on, and monitor, data protection impact assessments.
- cooperate with the ICO.
- be the first point of contact for the ICO and for individuals whose data is processed (employees, customers etc).

Disclosure of Data

Staff must not disclose personal data to any individual, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller or in line with the policy.

Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller or in line with the Data policy.

Before processing any personal data, all staff should consider the following:

- Do you really need to record the information?
- Is the information 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the individual been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?

Runway Training will also ask for information about health needs, such as allergies to forms of medication, or any conditions such as asthma or diabetes. Runway Training will only use the information in the protection of the health and safety of the individual but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff and learners will be asked to sign either an appropriate HR form or an individual document regarding types of information when an offer of employment or a course place is made. A refusal to sign such documents may result in the offer being withdrawn.

Awarding Organisations/Ofqual and Ofsted

In keeping with GDPR and Data Protection Act 2018, learners are informed during Induction of the personal data that is collected and processed and the purpose of doing so.

Learners are informed of information sharing between Runway Training and the Awarding body. All learners are asked to give consent to the sharing of this information.

In response to strengthening the security of the data processed between Runway Training and the Awarding Organisation, we ensure that relevant documents are password protected when sent.

By password-protecting documents containing personal or sensitive personal data, we can fortify our GDPR compliance effort and that of our centres.

Personal data and results may also be shared with Ofqual, Ofsted, the Institute for Apprenticeships and Technical Education (IfATE), and the End Point Assessment Organisation, which will be managed within the regulations laid down within the relevant legislation.

PICS and Altitude addition for data policy:

Sensitive learner and contract data are stored on PICS, an end-to-end apprenticeship management system as well as Altitude, an in-house system developed and maintained specifically for use at Runway Training by IsARC. Sensitive learner and contract data are stored here.

The Data and Compliance Team is responsible for user management - only those who need to use the system are given restricted permission to do so. Users must only be assigned permission to view the learners related to contracts that they exclusively work with.

When an individual leaves the organisation, their system permissions will immediately be revoked.

All data used off-platform is obfuscated and stored on a password-protected FTP server. The only people with access to this are on the Web Development Team or Data Team. IsARC is also able to access this data as they are responsible for the regular uploads to the FTP server.

Sharing of files between Runway Training and IsARC is done exclusively through an encrypted WhatsApp group, not via email.

The sharing of learner data must align with our data-sharing processes. Exporting of learner data is restricted by the system.

Subject Access Request Procedure

Purpose

This document outlines our policy for responding to subject access requests under the Data Protection Act (DPA).

Runway Training welcomes the rights of access to information that is set out in the DPA. We are committed to operating openly and meeting all reasonable requests for information not subject to specific exemptions in the Act.

How do you make a subject access request?

A subject access request is a written request for personal information (known as personal data) held about you by Runway Training. Generally, you have the right to see what personal information we hold about you. You are entitled to be given a description of the information, what

we use it for, who we might pass it onto and any information we might have about the source of the information. However, this right is subject to certain exemptions:

1. What do we do when we receive a subject access request?

Checking of identity

We will first check that we have enough information to verify your identity. Often, we will have no reason to doubt a person's identity. However, if we have good cause to doubt your identity, we can ask you to provide any evidence we reasonably need to confirm it.

If the person requesting the information is a relative/representative of the individual concerned, then the relative/representative is entitled to personal data about themselves but must supply the individual's consent for the release of their personal data.

Collation of information

We will check that we have enough information to find your requested records. If we need more information, we will promptly ask you for this. We will gather any manual or electronically held information and identify any information provided by a third party or which identifies a third party.

If we have identified information that relates to third parties, we will write to them asking whether there is any reason why this information should not be disclosed. We do not have to supply the information to you unless the other party has provided their consent, or it is reasonable to do so without their consent. If the third-party objects to the information being disclosed, we may seek legal advice on what action we should take.

Before sharing any information that relates to third parties, we will, where possible, anonymise information that identifies third parties not already known to the individual (e.g. the Authority employees) and revise information that might affect another party's privacy. We may also summarise information rather than provide a copy of the whole document. The DPA requires us to provide information, not documents.

Issuing our response

Once any queries about the information requested have been resolved, copies of the information in a permanent form will be sent to you except where you agree, where it is impossible, or where it would involve undue effort. In these cases, an alternative would be to allow you to view the information on screen at Runway offices.

We will explain any complex terms or abbreviations contained within the information when it is shared with you. Unless specified otherwise, we will also provide a copy of any information that you have seen before.

2. Will we charge a fee?

We can charge a maximum £10 fee. If we do charge a fee, we will inform you promptly of this.

3. **What is the timeframe for responding to subject access requests?**

We have 40 calendar days starting from when we have received all the information necessary to identify you, to identify the information requested, and any fee required, to provide you with the information or to provide an explanation about why we are unable to provide the information. In many cases, it will be possible to respond in advance of the 40-calendar day target and we will aim to do so where possible.

4. Are there any grounds we can rely on for not complying with a subject access request?

If you have made a previous subject access request, we must respond if a reasonable interval has elapsed since the previous request. A reasonable interval will be determined upon the nature

of the information, the time that has elapsed, and the number of changes that have occurred to the information since the last request.

5. **Exemptions**

The Act contains several exemptions to our duty to disclose personal data, and we may seek legal advice if we consider that they might apply. Possible exemptions would be information covered by legal professional privilege, information used for research, historical and statistical purposes, and confidential references.

If we agree that the information is inaccurate, we will correct it and, where practicable, destroy the inaccurate information. We will consider informing any relevant third party of the correction. If we disagree or are unable to decide whether the information is inaccurate, we will note the alleged error and keep this on file.

If you are unsatisfied with our actions, you can seek recourse through our complaints procedure. If you remain dissatisfied, you have the right to refer the matter to the Information Commissioner or seek recourse through the courts. The Information Commissioner can be contacted at: Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF T: 0303 123 1113 (local rate) or 01625 545 745 www.informationcommissioner.gov.uk

DOCUMENT BREACH NOTIFICATION PROCESS

Responsibilities

All members of Runway Training staff must report all suspected or possible breaches immediately they learn of them. Any data processors used by Runway Training are responsible for reporting breaches without unnecessary delay. Contracts with data processors should include terms to this effect.

Identification of a breach

Discovery of a possible breach

A possible breach may be discovered in several ways:

- By a Runway Training member of staff, contractor, employer, partner, alumnus or student.
- By automatic operation of breach detection tools
- By report from a data processor employed by Runway Training
- By report from a third party

Regardless of the means of discovery, the first Runway Training staff member to learn about a possible breach must report it immediately.

Reporting the breach

Reports should be made firstly to the DPO who will liaise with the appropriate member of the Senior Management team. If for any reason no member of the SMT are available, the report should be made to the Board of Governors.

Confirming the breach

Once a possible breach has been discovered, Runway Training may not immediately have a reasonable degree of certainty that an actual breach has occurred. In this case, we are allowed a short investigation period to establish what has occurred.

Once Runway Training has a reasonable degree of certainty that a breach has occurred, then:

- We must record and assess the breach.
- The clock starts on the 72-hour deadline for notifying the ICO.

Recording the breach

We must record the details of all breaches in the internal breach register. The DPO will maintain the register. The register should include:

- What happened
- What data was affected
- What individuals were affected
- What or who caused the breach
- The effects and consequences
- What do we plan to do to mitigate these effects and consequences
- A timeline of the breach, including when we first became aware of the incident and when we determined that it was a breach.
- Our decisions regarding notification

Assessing the risk

Assessment of the level of risk should consider:

- The type of breach
- The type of personal data
- The sensitivity of the personal data
- The volume of the personal data
- The number of affected individual(s)
- The nature of the processing.
- The ease of identifying individuals. For example, where data was encrypted, the risk is reduced.
- The severity of consequences for the individuals
- The permanence of consequences for the individuals
- Any special characteristics of the individuals. For example, are they children, or vulnerable persons?
- Where there is a breach of confidentiality, the intentions of the persons who have accessed the data.

The assessment should conclude that the breach is either:

- **Unlikely to result in a risk** to the rights and freedoms of natural persons.
- **Likely to result in a risk** to the rights and freedoms of natural persons.
- **Likely to result in a high risk** to the rights and freedoms of natural persons.

A Senior Manager should approve the assessment's conclusions.

Notification

The assessment of the likely risk determines what notifications are required:

- If the assessment is **"unlikely to result in a risk",** no notifications are required.
- If the assessment is **"likely to result in a risk",** then notification should be made to the ICO.
- If the assessment is **"likely to result in a high risk",** then notification should be made to both the ICO and the affected data subjects.

Note that the ICO has the power to require us to notify data subjects if they disagree with the risk assessment.

Timing of notifications

Where notification to the ICO or the data subjects is required, it should happen "without undue delay". In addition, notification to the ICO should happen within 72 hours of our becoming reasonably certain that a breach has occurred. If we take longer than 72 hours to notify the ICO, we must provide reasons for the delay.

It is acceptable to submit a partial notification to meet the 72-hour deadline and update it later. Such a partial notification should be clear that it is partial, include information about the potential scope of the breach and its consequences, and describe our plans to deal with the breach.

Use of data processors

If we are the controller of a processing activity but use a data processor to do the work, we still have the same responsibilities.

If a data processor becomes aware of a possible breach, they are allowed a short investigation period to confirm. Once they become reasonably certain that a breach has occurred, they are required by the GDPR to notify us without undue delay.

Note that in such a case, the 72-hour clock begins when Runway Training is notified of the breach by the data processor.

Notification to the ICO

The Data Protection Officer should make the notification. The notification should be made without undue delay and within 72 hours of confirmation of the breach. It should include:

- Details of the breach, including the categories and approximate numbers of data subjects and data records involved.
- Contact details for the DPO or some other appropriate contact point.
- The likely consequences of the breach.
- The measures already taken or proposed to address the breach and mitigate possible adverse effects.

As mentioned above, if the notification is made more than 72 hours after we became aware of the breach, we must also provide reasons for the delay.

Notification to the Data Subject

The Data Protection Officer should make the notification.

The notification should be made without undue delay and include the following:

- A description of the breach.
- Contact details for the DPO or some other appropriate contact point.
- A description of the likely consequences for the subject.
- A description of the measures already taken or proposed to address the breach and mitigate its possible effects.

Where appropriate, we should also advise the data subjects on steps they can take to protect themselves. The notification should stand alone and not be sent with other information, such as in a newsletter. Generally, we should choose the communication method or methods we believe will be most effective. If it would be disproportionately difficult to notify each data subject directly, then we can do so via a prominent public announcement.

Data Portability

The Company provides all personal information pertaining to the data subject to them on request and in a format that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

To ensure that we comply with Article 20 of the data protection laws concerning data portability, we keep a commonly used and machine-readable format of personal information where the processing is based on: -

- Consent pursuant to point (a) of Article 6(1)
- Consent pursuant to point (a) of Article 9(2)
- A contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means

Where requested by a data subject and if the criteria meet the above conditions, we will transmit the personal data directly from the Company to a designated controller, where technically feasible.

We utilise the below formats for the machine-readable data: -

- HTML
- CSV
- XML
- RDF
- XHTML

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

DATA BREACH INCIDENT FORM (*TEMPLATE*)

DPO/COMPLIANCE OFFICER/INVESTIGATOR DETAILS:			
NAME:		**POSITION:**	
DATE:		**TIME:**	
TEL:		**EMAIL:**	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH:			
CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO. OF DATA SUBJECTS AFFECTED:		**NO. OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			

BREACH NOTIFICATIONS:		
WAS THE SUPERVISORY AUTHORITY NOTIFIED?	**YES/NO**	
IF YES, WAS THIS WITHIN 72 HOURS?	**YES/NO/NA**	
If no to the above, provide reason(s) for delay.		
WAS THE BELOW INFORMATION PROVIDED? *(if applicable)*	**YES**	**NO**
A description of the nature of the personal data breach		
The categories and approximate number of data subjects affected		
The categories and approximate number of personal data records concerned		
The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information)		
A description of the likely consequences of the personal data breach		
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)		
WAS NOTIFICATION PROVIDED TO DATA SUBJECT?	**YES/NO**	
INVESTIGATION INFORMATION & OUTCOME ACTIONS:		
DETAILS OF INCIDENT INVESTIGATION:		
PROCEDURE(S) REVISED DUE TO BREACH:		
STAFF TRAINING PROVIDED: *(if applicable)*		

DETAILS OF ACTIONS TAKEN AND INVESTIGATION OUTCOMES:

HAVE THE MITIGATING ACTIONS PRVENTED THE BREACH FROM OCCURRING AGAIN? *(Describe)*

WERE APPROPRIATE TECHNICAL MEASURES IN PLACE?	**YES/NO**
If yes to the above, describe measures.	

SIGNATURES	
Investigator Signature: _____	Date: _____
Investigator Name: _____	Authorised by: _____

DATA RETENTION & ERASURE PROCEDURE

Effective and adequate records and data management is necessary to: -

- Support core business functions and provide evidence of conduct and the appropriate maintenance of systems, tools, resources and processes.
- Meet legislative, statutory and regulatory requirements.
- Assist in document policy formation and managerial decision making.
- Provide continuity in the event of a disaster or security breach.
- Protection personal information and data subject rights
- Avoid inaccurate or misleading data and minimise risks to personal information.
- Erase data in accordance with the legislative and regulatory requirements

Information held for longer than is necessary carries additional risk and cost and can breach data protection rules and principles.

We define ***'records'*** as all documents, regardless of the format, which facilitate business activities, and are thereafter retained to provide evidence of transactions and functions.

Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations.. However, we are committed to collecting, processing, storing and destroying all information in accordance with the requirements of the ***General Data Protection Regulation (GDPR)***, the ***Data Protection Act 2018 (DPA18)*** and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

Our Data Retention Policy and processes comply fully with the GDPR's fifth Article 5 principle: -

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes as per Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation to safeguard the rights and freedoms of the data subject **('storage limitation').**

Objectives

A record is information, regardless of media, created, received, and maintained which evidences the development of, and compliance with, regulatory requirements, business practices, legal policies, financial transactions, administrative activities, business decisions or agreed actions. It is the Company's objective to implement the necessary records management procedures and systems which assess and manage the following processes: -

- The creation and capture of records
- Compliance with legal, regulatory and contractual requirements
- The storage of records
- The protection of record integrity and authenticity
- The use of records and the information contained therein
- The security of records
- Access to and disposal of records

Records contain information that are a unique and invaluable resource to the Company and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information contained in them, as well as the individuals such information refers to. Records are also pivotal in the documentation and evidence of all business functions and activities.

Guidelines & Procedures

The Company manage records efficiently and systematically, in a manner consistent with the GDPR requirements, ISO15489 and regulatory Codes of Practice on Records Management. Records management training is mandatory for all staff as part of the Company's statutory and compliance training programme and this policy is widely disseminated to ensure a standardised approach to data retention and records management.

Records will be created, maintained and retained to provide information about, and evidence of the Company's transactions, customers, employment and activities. Retention schedules will govern the period that records will be retained and can be found in the ***Record Retention Periods*** table at the end of this document.

Retention Period Protocols

All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All company and employee information are retained, stored and destroyed as per legislative and regulatory guidelines.

For all data and records obtained, used and stored within the Company, we: -

- Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain
- Establish periodical reviews of data retained
- Establish and verify retention periods for the data, with special consideration given to the following areas: -
    - the requirements of the Company
    - the requirements of our funding bodies
    - the type of personal data
    - the purpose of processing
    - lawful basis for processing
    - the categories of data subjects

- Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, the Company will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices
- Have processes in place to ensure that records pending audit, litigation or investigation are not destroyed or altered
- Transfer paper-based records and data to an alternative media format in instances of long retention periods (*with the lifespan of the media and the ability to migrate data where necessary always being considered*)

Designated Owners

All systems and records have designated owners (IAO) throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Owners are assigned based on role, business area and level of access to the data required. The designated owner is recorded on the Retention Register and is fully accessible to all employees. Data and records are never reviewed, removed, accessed or destroyed with the prior authorisation and knowledge of the designated owner.

Document Classification

The Company have detailed Asset Management protocols for identifying, classifying, managing, recording and coordinating the Company's assets (*including information*) to ensure their security and the continued protection of any confidential data they store or give access to. We utilise an ***Information Asset Register (IAR)*** to document and categorise the assets under our remit and carry out regular Information Audits to identify, review and document all data flows within the Company.

We also carry out regular Information Audits, which enable us to identify, categorise and record all personal information obtained, processed and shared by our company in our capacity as a controller and processor and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Retention periods
- Access level (*i.e. full, partial, restricted etc.*)

Our information audits and registers enable us to assign classifications to all records and data, thus ensuring that we are aware of the purpose, risks, regulations and requirements for all data types.

We utilise 5 main classification types: -

1. **Unclassified** - information not of value and/or retained for a limited period where classification is not required or necessary.
2. **Public** - information that is freely obtained from the public and as such, is not classified as being personal or confidential.
3. **Internal** - information that is solely for internal use and does not process external information or permit external access.
4. **Personal** - information or a system that processes information that belongs to an individual and is classed as personal under the data protection laws.
5. **Confidential** - private information or systems that must be secured at the highest level and are afforded access restrictions and high user authentication.

The classification is used to decide what access restriction needs to be applied and the level of protection afforded to the record or data. The classification along with the asset type, content and description are then used to assess the risk level associated with the information and mitigating action can then be applied.

Suspension of Record Disposal for Litigation or Claims

If the Company is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against our firm, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

Storage & Access of Records and Data

Documents are grouped together by category, clear date and alphabetical order when stored and/or archived. Documents are always retained in a secure location, with authorised personnel being the only ones to have access. Once the retention period has elapsed, the documents are reviewed, archived or confidentially destroyed depending on their purpose, classification and action type.

Expiration of Retention Period

Once a record or data has reached its designated retention period date, the designated owner should refer to the retention register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes, it is sufficient to anonymise the data following the GDPR requirements or to archive records for a further period.

Destruction and Disposal of Records & Data

All information of a confidential or sensitive nature on paper, card, microfiche or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, clients and customers.

The Company is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions of the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

Paper Records

Due to the nature of our business, the Company retains paper-based personal information and, as such, must ensure that it is disposed of in a secure, confidential and compliant manner. The company utilise a professional Shredding Service Provider to dispose of all paper materials.

These are stored securely in the office in a locked 'post box', where sensitive documents etc. can only be posted in but not then taken out without a key, held by the office manager.

Regular collections take place by the professional Shredding Service Provider to ensure that confidential data is disposed of appropriately.

Electronic & IT Records and Systems

When records or data files are identified for disposal, their details must be provided to the designated owner to maintain an effective and up-to-date register of destroyed records.

Where possible, information is wiped from the equipment through the use of software and formatting. However, this can still leave imprints or personal information that is accessible, and so we also comply with the secure disposal of all assets by using government approved software erasure processes to avoid this.

Internal Correspondence and General Memoranda

Unless otherwise stated in this policy or the retention periods register, correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support *(i.e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed*).

Where correspondence or memoranda that do not pertain to any documents having already been assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content cease or, at a maximum, two years.

Examples of correspondence and routine memoranda include (but are not limited to): -

- Internal emails
- Meeting notes and agendas
- General inquiries and replies
- Letter, notes or emails of inconsequential subject matter

Erasure

In specific circumstances, data subjects have the right to request that their personal data be erased. However, the Company recognises this is not an absolute *'right to be forgotten'*. Data subjects only have a right to have personal data erased and to prevent processing if one of the *below conditions applies: -*

- Where the personal data is no longer necessary concerning the purpose for which it was initially collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest in continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Where one of the above conditions apply and the Company received a request to erase data, we first ensure that no other legal obligation or legitimate interest apply.

These measures enable us to comply with a data subject's right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its

continued processing. Whilst our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed: -

1. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -
    a. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
    b. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
    c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing
    d. the personal data has been unlawfully processed
    e. the personal data must be erased for compliance with a legal obligation
    f. the personal data has been collected in relation to the offer of information society services to a child
2. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
3. Where the Company has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If, for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and a judicial remedy. ***Such refusals to erase data include: -***

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest relating to public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims

Special Category Data

In accordance with GDPR requirements and Schedule 1 Part 4 of The Data Protection Act 2018, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data and criminal convictions etc.

Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, as noted on our retention register schedule.

Compliance and Monitoring

The Company are committed to ensuring continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving and retention.

Retention Register

The retention register below pertains to all documentation except ESF documentation where retention rates will be as follows depending on funding start dates:

2021: All project documents will be kept for 10 years after the final ESF claim is paid by the ESF Managing Authority and the Managing Authority will be consulted before records are disposed of.

Pre 2021: All ESF documents will be retained until 31 December 2034 and at that point of the document retention date, before ESF project documentation is destroyed a check will be made of the GOV.UK website and/or the Managing Authority to ensure it is safe to do so.

RECORD	RETENTION PERIOD	ASSET OFFICER	ACTION	NOTES
Information, data or record	*Period for retaining record & accompanying notes*	*Who is responsible for reviewing periods*	*Destroy, archive, review etc.*	
Accident books, accident records/reports	3 years from last entry			
Accounting records	3 years for private companies 6 years for public limited companies			
Income tax and NI returns Income tax records IR correspondence	At least 3 years after the end of the financial year to which they relate			
Records of tests & examinations of control systems and protective equipment under COSHH	5 years from the date of the test			
Statutory Maternity Pay records, calculations, certificates & related medical evidence	3 years after the end of the tax year in which the maternity period ends			
Wage/salary records, overtime, bonus & expenses	6 years			
National minimum wage records	3 years + current year after the end of the pay reference period			
Application forms and interview notes (*for unsuccessful candidates)*	1 year from date of interview			

Personnel files and training records *(including recruitment, disciplinary records and working time records)*	6 years after date employment ceases			
RECORD	**RETENTION PERIOD**	**ASSET OFFICER**	**ACTION**	**NOTES**
Redundancy details, calculations of payments & refunds	6 years from the date of redundancy			
Statutory Sick Pay records, calculations, certificates & self-certificates	6 years			
Complaints, records, letters, responses & customer communications received by an FCA regulated firm	5 years for complaints relating to MiFID business or collective portfolio management services 3 years for all other complaints			
Records documenting the firm's relationships and responsibilities to statutory and/or regulatory bodies and its legal responsibilities	Permanent			
Business documents, policies, procedures, strategies etc.	Superseded + 6 years *(then reviewed for archive value purposes)*			
Supplier, business relationship documents, contracts, SLA's, audits, reviews etc.	End of relationship + 6 years			
Reviews, analysis, compliance monitoring, quality assurance, operational performance etc.	5 years +1			
Marketing, promotion, press releases	2 years after last action			
Memberships, certification and/or accreditation with professional associations	End of membership/accreditation + 1 year			