


Document title:	Data Protection and GDPR Policy	Date of Issue:	31/3/2023	Date for review	13/04/2024
Owner:	Beverley Ellis	Issue Number:	23-2	Previous Version:	23-2
This policy has been reviewed and approved by the Operations Director:					 Beverley Ellis

1. Policy Statement

- 1.1. TRS Training Limited are committed to compliance with the Data Protection Act 2018. We treat personal data that we hold respectfully, ensuring that we follow the principles of the Data Protection Act 2018 through our day to day duties and apply a duty of confidence of personal data.

2. Scope of Policy

- 2.1. This policy applies to all of TRS Training Limited's data processing and data controlling functions, including those performed on applicants', learners', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.
- 2.2. Partners and any third parties working with or for TRS Training Limited, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy.
- 2.3. This policy does not apply in the instances of dealing with a safeguarding issue or the reporting of an individual to the DBS service or a referral to the barred list, and in those circumstances, TRS would act in accordance to the Keeping Children Safe in Education 2021 guidance.

3. TRS Values

This policy underpins our commitment to our values, with particular reference to:

- RESPECT – All individuals and their unique talents
- RESPOND – Listening to our customers, partners and stakeholders and being equipped to meet their changing needs
- PARTNERS – Developing sustainable partnerships where everyone involved benefits from the relationship
- QUALITY – Providing outstanding teaching, learning and customer service

4. Implementation Principles

- 4.1. TRS Training Limited is a data controller and data processor in relation to data protection regulations.
- 4.2. TRS Training processes and controls data in accordance with the Data Protection Act 2018, ensuring information is:
 - used fairly, lawfully and transparently
 - used for specified, explicit purposes
 - used in a way that is adequate, relevant and limited to only what is necessary
 - accurate and, where necessary, kept up to date
 - kept for no longer than is necessary
 - handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage
- 4.3. Data subjects may make data access requests as described in Subject Access Request Procedure (Appendix 2). We recognise data subjects' rights to find out what information we store about them, including the right to:
 - be informed about how their data is being used
 - access personal data
 - have incorrect data updated
 - have data erased
 - stop or restrict the processing of their data

- data portability (allowing them to get and reuse their data for different services)
 - object to how their data is processed in certain circumstances
- 4.4. The Data Privacy Notice gives details of the data that is collected, processed and controlled by TRS Training and its purposes. (Appendix 1).
- 4.5. Data subjects have the right to complain to TRS Training Limited about any issue related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Comments, Compliments and Complaints Procedure.
- 4.6. Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, TRS Training Limited shall, prior to the processing, carry out a Data Protection Impact Assessment (DPIA) of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.
- 4.7. Where, as a result of a DPIA it is clear that TRS Training Limited is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not TRS Training Limited may proceed must be approved by the Board, who in turn may refer this to the ICO. Appropriate controls will be applied to reduce the level of risk associated with processing individual data to an acceptable level in compliance with the GDPR.

Disclosure of Data

- 4.8. TRS Training Limited does not disclose personal data to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff exercise caution when asked to disclose personal data held on another individual to a third party, and only do so when authorised to do so and it is considered relevant and necessary for the conduct of our business.

Consent

- 4.9. TRS Training Limited understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time by contacting compliance@trstraining.net.
- 4.10. TRS Training Limited understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.
- 4.11. All applicants and client enquiries are given the option to "opt out" of marketing and further contact from TRS. Their choices are understood and must be followed by all members of staff.
- 4.12. Lead generation campaigns include what data will be collected, how this will be used and how long it is stored for. Options to "opt out" of this data collection is provided for each campaign.
- 4.13. For learners, consent to collect and process personal data is requested at enrolment. Employers agree to this in the Contracts for Services agreement.
- 4.14. For sensitive data, explicit written consent of data subjects is to be obtained unless an alternative legitimate basis for processing exists.

Security of Data

- 4.15. All staff are responsible for ensuring that any personal data that TRS Training Limited holds and for which they are responsible, is kept securely and is not disclosed to any third party unless that third party has been specifically authorised by TRS Training Limited to receive that information and has entered into a confidentiality agreement.
- 4.16. All personal data is accessible only to those who need to use it, and access may only be granted by a member of the senior management team and for a specific purpose. Access is monitored using the User Access Register. All personal data is treated with the highest security and is kept:
- in a lockable room with controlled access; and/or
 - in a locked drawer or filing cabinet; and/or

- if computerised, password protected;

- 4.17. TRS does not authorise personal data being stored on removable computer media, even if this is encrypted.
- 4.18. Manual records are not left where they can be accessed by unauthorised individuals and may not be removed from business premises without explicit authorisation. Staff must take extra care when collecting data off premises for the purposes of enrolment, or other similar functions, to ensure the security of the data. Data must not be kept in vulnerable areas for any long periods, this includes cars, laptop bags or files in public areas.
- 4.19. As soon as manual records are no longer required for day-to-day use, they are removed to secure archiving. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'.

Retention and Disposal of Data

- 4.20. TRS Training Limited does not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected. Please see Appendix D for retention durations.
- 4.21. TRS Training Limited may store data for longer periods if the personal data will be processed solely for statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.
- 4.22. Leads generated through marketing activities and applications that are received by TRS will be held for 6 months, they will then either have been processed through the normal applications process or will all the data will deleted.
- 4.23. Personal data is disposed of securely in accordance with data protection regulations.
- 4.24. Personal data is retained for the following terms:
 - Staff records are destroyed after 6 years from the employee's leave date
 - DBS records are destroyed within six months of receipt, the DBS number is kept until a renewal is required, and for 6 years after the staff member has left TRS Training Ltd
 - Learner personal records are kept for the contractually determined period of the Education and Skills Funding Agency (ESFA) and European Social Fund (ESF) in line with Apprenticeship Funding Rules
 - Complaints are kept for as long as we reasonably consider that a data subject may legally bring an additional or repeat claim against us.
- 4.25. Safeguarding records are kept for 6 years from the date the learner left TRS Training Ltd and are disposed of securely and confidentially.
- 4.26. All staff are trained on the Data Protection Act 2018 as part of the induction process, and receive regular training updates at least every two years.
- 4.27. Employers' intellectual property rights which may be observed through training activities are respectfully kept confidential by trainers and evidence of these are signposted rather than kept as hard copies, and any references documented in learners' work are redacted.
- 4.28. Any breach of this policy will be dealt with under TRS Training Limited's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.
- 4.29. All staff observe the clear desk guidance (Appendix 3), Willful failure to adhere to this guidance or a clear lack of care to securely and sensitively handle data will be treated as gross misconduct.
- 4.30. If there is breach that requires us to report the incident to the ICO we will do so within 72 hours.

5. Roles and Responsibilities

- 5.1. Our ICO registration number is ZA123990 - Our DPO can be contacted at compliance@trstraining.net
- 5.2. Those in managerial or supervisory roles throughout TRS Training Limited are responsible for developing and encouraging good information handling practices within TRS Training Limited by TRS staff.

- 5.3. The Senior Management are responsible for TRS Training Limited's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that TRS Training Limited complies with the GDPR, as do those in respect of data processing that takes place within their area of responsibility.
- 5.4. The Senior Management Team are responsible for implementing and overseeing the Subject Access Request Procedure and are the first point of call for seeking clarification on any aspect of data protection compliance.
- 5.5. Compliance with data protection legislation is the responsibility of all learners, employers, stakeholders, partners, contractors and staff of TRS Training Limited who process personal data.
- 5.6. All learners, employers, staff, partners and stakeholders of TRS Training Limited are responsible for ensuring that any All personal data about them and supplied by them to TRS Training Limited is accurate and up-to-date.

6. Policy Monitoring and reporting arrangements

- 6.1. The Senior Management Team are responsible for reviewing the Data Inventory annually in the light of any changes to TRS Training Limited's activities and to any additional requirements identified by means of data protection impact assessments.
- 6.2. The Board will review any Subject Access Requests as part of Strategic Objective 1.
- 6.3. The Board are responsible for approving this policy
- 6.4. The policy is reviewed annually.

7. Summary of Revisions

Version	Date	Revision
23-2	31/3/23	Added details about how we process and store data for applicants and lead generated from marketing campaigns with Data Retention
23-2	31/3/23	Added details about including the choice to "opt out" from data collection for applicants and leads generated from marketing campaigns with Consent
22-1	12/01/2023	Changed Quality Manager to Head of Department in line with structural staff changes.
22-1	12/01/2023	Approved for use by Operations Director

Data Privacy Notice (Appendix 1)

1. Scope:

All learners, whose personal data is collected, in line with the requirements of the GDPR, are data subjects.

2. Responsibilities:

The Data Protection Officer is responsible for ensuring that this notice is made available to data subjects prior to TRS Training collecting/processing their personal data.

All staff at TRS, who interact with data subjects, are responsible for ensuring that this notice is drawn to the data subject's attention and their consent to the processing of their data is secured.

3. Privacy Notice:

How to contact us?

Our Data Protection Office and data protection representatives can be contacted directly by telephone on 01744 809010 or at compliance@trstraining.net

3.1 The personal data we would like to collect from you is:

Personal data type:	Source: (where we obtained the personal data from, if it has not been collected directly from you):
<ul style="list-style-type: none"> personal details (name, address, post code, date of birth, age, gender, national insurance number, ULN, contact numbers, email address) nationality and residency information residency card information Ethnicity household information details of previous qualifications, employment and educational history employment details (company information, contracted hours of employment, length of employment, current job roles and duties) unemployment details (length of unemployment, benefit claimed, benefit office) additional needs (learning difficulty and/or disability) other health, wellbeing and/or medical issues (such as mental health, other medical conditions, medication details) education, health and care plan information additional support needs information family details (parents/ carers/ guardians for under 18's and emergency contact information) Learner Records Service information Personal, career and progression objectives IAG outcomes attendance information (sessions attended, absences, reasons for absences) progression and achievement information client interview record information visual images (CCTV, photographs) 	<p>Your employer</p> <p>Learner Records Service</p>

- offences and alleged offences
- criminal proceedings, outcomes and sentences
- external support services/ specialist services (such as Probation, Mental Health and Health care services, Drug and Alcohol services, leaving care support services, Social Services)

Multi-agency partners

The personal data we collect will be used for the following purposes:

- Learner Records Management
- Examinations and Achievement
- Safeguarding
- Funding Claims
- Learner Support
- Learning - IT Systems (Onefile, email, storage, e-learning)
- Marketing and publicity

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the GDPR. What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

- family, associates and representatives of the person whose personal data we are processing
- professional advisers
- current or prospective employers
- examining bodies (awarding organisations)
- trade, employer and professional organisations
- ESFA
- DWP
- LRS
- Healthcare, social and welfare organisations
- local and central government
- survey organisations
- persons making an enquiry or complaint
- financial organisations
- Careers Service
- Counter Terrorism Police
- Local press and media
- Police forces and probation services
- Community organisations

TRS processes data in order to fulfil contractual obligations such as:

- Education and Skills Funding Agency (ESFA)
- European Social Fund (ESF)
- Learner Records Service
- DWP as a Kickstart Intermediary Organisation
- Awarding Organisations and End Point Assessment Organisations
- Healthcare, social and welfare organisations
- Police and Probation
- Local and central government

3.2 Consent

By consenting to this privacy notice you are giving us, TRS Training Ltd, permission to process your personal data specifically for the purposes identified.

Consent is required for TRS to process both types of personal data but it must be explicitly given. Where we are asking you for sensitive personal data we will always tell you why and how the information will be used.

You may withdraw consent at any time by emailing compliance@trstraining.net.

3.3 Disclosure

TRS will not pass on your personal data to third parties without first obtaining your consent. The following third parties will receive your personal data for the following purpose(s) as part of the processing activities:

Third Party Organisation:	Safeguards in place to protect your personal data:	Access to safeguards in place:
Awarding organisations and EPAs (Edexcel, City and Guilds, EAL, RHA, ILM, Skills for Logistics)	Authorised access via password	
ACE 360	Authorised access via password	
PICS	Authorised access via password	
Onefile	Onefile: ISO 27001 (Information Security Standard)	https://www.onefile.co.uk/policies/information-security-policy/index.html
ESFA and LRS	The security of the ESFA's systems which process and store data are regularly reviewed in accordance with Government requirements, and assessments and checks promoted by the Information Commissioner's Office. Data is securely deleted when it is no longer required for the purposes collected.	www.gov.uk/government/publications/esfa-privacy-notice www.gov.uk/government/publications/lrs-privacy-notice
DWP	All personal data on 'Apply for a Kickstart Scheme Grant for Employers' is processed, stored and managed entirely in the European Economic Area (EEA), and will not be transferred outside of it. This means that it is covered by EU Data Protection regulations.	https://www.apply-kickstart-grant-employer.service.gov.uk/privacy-policy
Local Safeguarding Boards and Counter Terrorism Police	Authorised access via password	

3.4 Retention Period:

TRS will process personal data whilst you are a learner and will store the personal data for a number of years. The retention period for different classifications of personal data has been established in line with information management guidelines.

3.5 Your rights as a data subject

At any point while we are in possession of, or processing your personal data, you, the data subject, have the following rights:

- Right of access – you have the right to request a copy of the information that we hold about you.
- Right of rectification – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- Right to be forgotten – in certain circumstances you can ask for the data we hold about you to be erased from our records.

-
- Right to restriction of processing – where certain conditions apply to have a right to restrict the processing.
 - Right of portability – you have the right to have the data we hold about you transferred to another organisation.
 - Right to object – you have the right to object to certain types of processing such as direct marketing.
 - Right to object to automated processing, including profiling – you also have the right to be subject to the legal effects of automated processing or profiling.
 - Right to judicial review: in the event that TRS refuses your request under rights of access, we will provide you with a reason as to why. You have the right to complain as outlined in clause 3.6 below.

All of the above requests will be forwarded on should there be a third party involved (as stated in 3.4 above) in the processing of your personal data.

3.6 Complaints

In the event that you wish to make a complaint about how your personal data is being processed by TRS (or third parties as described in 3.4 above), or how your complaint has been handled, you have the right to lodge a complaint directly with the supervisory authority and TRS's Data Protection Officer.

(Appendix 2)

Subject Access Request Procedure

You have the right to request for personal data we may hold about you. This is known as a Data Subject Access Request ("DSAR"). A data subject is an individual who is the subject of the personal data. If you wish to make a DSAR, please complete this form and return to us by post or email.

If sending by post, please use the following address:

Data Protection Officer
 TRS Training Limited
 Unit 4 Micklehead Business Village
 St Michaels Road
 Sutton Manor
 St Helens
 Merseyside
 WA9 4YU

If sending by email, please send to compliance@trstraining.net

1. Data Subject's Full Name:		2. Data Subject's Date of Birth:	
3. Data Subject's Current Address :			
4. Data Subject's Telephone Number:			
Home Telephone No:		Mobile Telephone No:	
5. Details of data requested:			
6. To help us search for the information you require, please let us know the data you require with as much detail as possible (e.g. copies of emails between <date> and <date>). If we do not receive sufficient information to locate the data you require, we may be unable to comply with your request			

7. Is the information going to be sent to the data subject or his/her representative?

To the data subject ☐ To the representative ☐

If the data is sent to the representative, then sections 9 and 10 need to be filled out.

8. I confirm that I am the Data Subject.

Signature: _____

Print Name: _____

Date: _____

I enclose a copy of my ID and address proof documents (including a government issued ID document).

9. (To be filled out if the question 7 is answered with "To the representative") The Data Subject (whose data is being requested) must give written authorization for the information to be released to his/her authorized representative.

I hereby give my authorization for _____
(fill out the name of the authorized representative) to request access to my personal data.

Signature of Data Subject: _____

Print name: _____

10. (To be filled out by the representative of the data subject) I confirm that I am the authorized representative of the Data Subject.

Name of authorized representative and address where personal data is to be sent:

Signature: _____

Print Name: _____

Date: _____

We will acknowledge receipt of your request, and will aim to process your data subject access request within 5 days, but not more 30 days. However, if you have any queries whilst your request is being processed, please do not hesitate to contact us at this email address: compliance@trstraining.net.

CLEAR DESK GUIDANCE (Appendix 3)

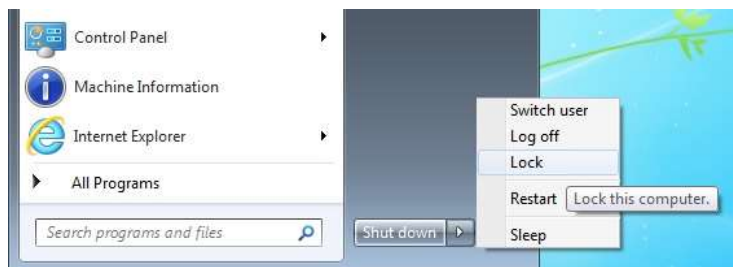
Whether you have an allocated desk, an office or work in a hot desk area, maintaining a clear desk supports security, cleanliness and allows others to easily use available space. Adopting a clear desk approach will help reduce the risk of unauthorised access to sensitive and confidential documents and data.

PLAN first thing in the morning. Keep just the things you need for your workday on your desk. File all other folders and documents in locked storage, but don't leave the key in!

PROTECT information whenever you leave your desk. Do not leave confidential or sensitive information unattended on your desk, lock it away, or lock your office door. In addition, if you are not taking your device with you, lock it using one of the following:

For Windows Users

- pressing the **Window and L keys** at the same time
- pressing **Ctrl + Alt + Delete** keys at the same time and choosing the "Lock this Computer" or "Lock" option
- or by using the function from the start menu



For Mac Users - To lock your Mac's screen, simultaneously press the following keys: **Control + Shift + Eject**.



If you have a newer Mac that does not have an optical drive (and so has no eject key on the keyboard), the command is **Control + Shift + Power**. In both cases, you'll see your Mac's display shut off immediately, while the system continues to run in the background.

PICK UP at the end of the day. When you leave in the evening, don't leave documents out or whiteboards with information or data on them. It is essential to file away your documents in locked storage or shred them.

FAQs for clear desk

How do I lock my screen before I move away from my device?

- Pressing the Window-L keys together, the Ctrl-Alt-Delete keys at the same time and choosing the "Lock this Computer" or "Lock" option or by using the function from the start menu.

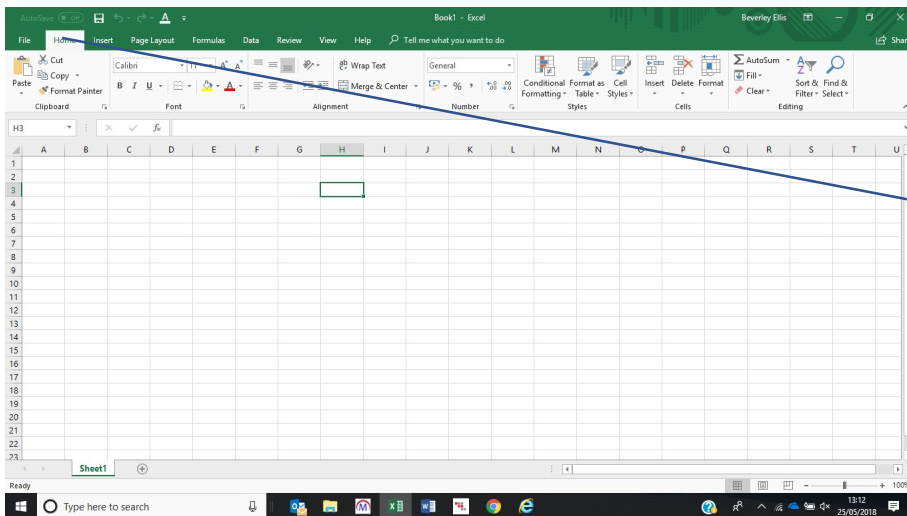
I don't have any personal filing space, what should I do?

- All personal filing and items should be locked away each night into your allocated space. If you do not have personal or team filing speak with your line manager.

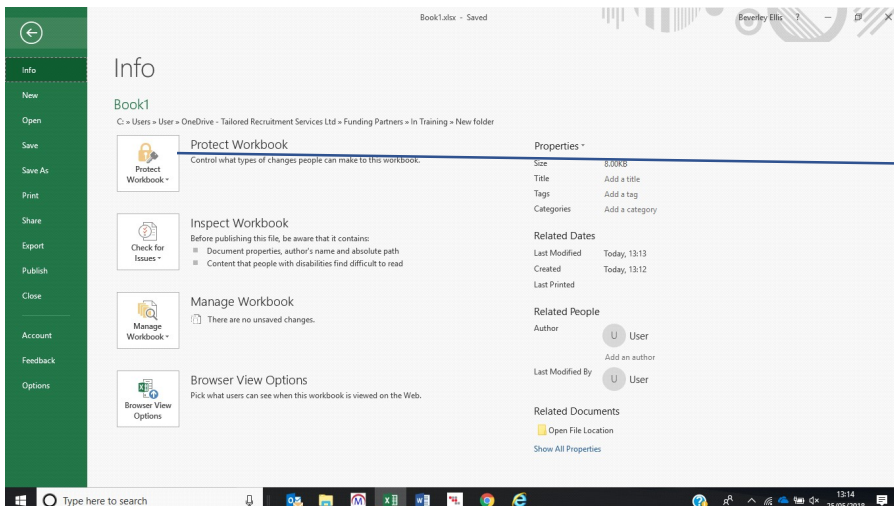
We do not have enough storage for the team, what should we do?

- You should review your storage needs regularly. When staff leave keys should be passed back to their line/office managers who should arrange for these to be reallocated or retained centrally within your team. If you do not have enough storage (or have too much) talk to your line manager.

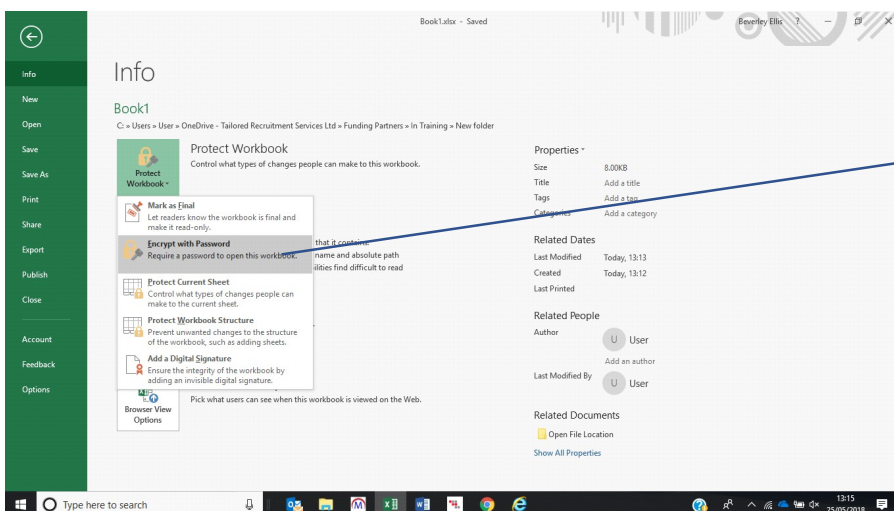
HOW TO PASSWORD PROTECT A SPREADSHEET



Click on "File"
Save the document
Click back on "File"



Click "Protect
Workbook"



Click "Encrypt with
Password"

1. Introduction to record keeping

As an ESFA provider, you must hold evidence to assure us that you are using ESFA funding appropriately.

You must also meet UK GDPR and Data Protection Act 2018 requirements in relation to data sharing and data protection, see the [Information Commissioners Office \(ICO\) guide to data protection](#) for details.

When your contract with ESFA ends, you must ensure your learner records are transferred to ESFA if required and all other records are either securely destroyed if they have reached their retention period or retained by you until their destruction date is reached.

2. What is the minimum that should be kept?

As a minimum you should keep a learner file for each learner. It should contain:

- evidence about the learner, e.g. proof of identify
- evidence of eligibility for funding
- evidence of qualifications/course studied and achieved
- European Social Fund (ESF) financial information – as detailed in ESF guidance (if applicable)

See the [provider rules](#) for more details of what should be retained in the learner file.

For learner files relating to **ESF training provision**, you and your subcontractors **must** follow the retention of documents guidance as detailed in the [ESF 2014 to 2020 funding rules](#).

3. How should files be stored?

It is recommended that learner files should be stored electronically. Electronic data records and documents should be stored in secure off-site cloud-based servers that meet accepted security standards and legal requirements so can be relied upon for audit purposes (including ISO 27001).

However, if records are kept in paper-format they should be stored in individual wallets, one wallet per learner per academic year. All paper records should be stored in secure, lockable, fireproof, non-portable storage containers and access should be strictly controlled and limited to staff that need to access the records.

It is recommended that learner files should be stored in electronic systems or paper wallets that contains the following information:

- learner's surname, first name
- course studied
- academic year
- ESF contract number (if applicable)
- destruction date (6 years from date study ended, or 31/12/2030 if ESF-funded)

ESF records must be easily identifiable and it is recommended that they are kept separately.

4. Transfer of records

If the learner moves to a new provider or the contract is terminated, you must:

- retain their learner file as per retention periods in section 5. The new provider will gather new evidence for the learner.
- transfer their portfolio so they can continue their course with the new provider.

If the learner file needs to be transferred back to ESFA, the ESFA record transfer agreement should be used.

Paper learner files should be boxed up keeping ESF records in separate boxes. Files should be weeded before boxing, i.e. remove duplicate documents, remove plastic wallets and secure all records in the relevant learner's wallet.

5. Retention of records

Learner files should be retained securely for 6 years from Financial Year End after end of course or until 31/12/2030 if ESF-funded provision.

This guidance is in addition to the statutory guidance provided by [Companies House](#) and [HMRC](#) on a company's record keeping requirements.

The ICO also provides guidance on [document retention requirements](#).

5.1 Record checklist

Type of record	Retention period	Action	Completed
Learner records: <ul style="list-style-type: none"> • Details of learner • Course studied • Learner eligibility 	6 years from Financial Year End after last payment made	Destroy records older than 7 years. List all remaining records with full name, course studied & course dates.	
'Live' Portfolios (paper and electronic)*	2 years from end of course	Destroy records older than 2 years. List all remaining records with full name, course studied & course dates.	
Certificates	N/A - send to learner	Return all certificates to awarding body if not sent to learner.	
European Social Fund (ESF)	For the 2007-13 ESF Programme this is expected to be until at least 31 December 2022. For the For the 2014-20 ESF Programme until at least 31 December 2030.	Destroy records if past destruction date. List all remaining records with full name, course studied and course dates. Note: check the DWP - ESF guidance before destroying any paperwork in case the destruction date has changed.	
Corporate records: <ul style="list-style-type: none"> • HR records • Finance records • Contract records 	Retain as per statutory guidance provided by Companies House and HMRC on a company's record keeping requirements		

***Note:** these are the Portfolios that relate to current learning and certificates haven't been claimed

6. Disposal of records

When records have reached their retention period, data will be disposed of securely and confidentially.

All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable:

- paper records should be shredded using a cross-cutting shredder or shredded by an external company.
- CDs / DVDs / floppy disks should be cut into pieces
- audio / video tapes and fax rolls should be dismantled and shredded
- hard disks should be dismantled and sanded

Do not put records in with the regular waste or a skip.

Note: Where an external contractor is used for shredding records, it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.