Central Training Group

Data Protection Policy
2024 – 2025

Includes

Privacy Notice

Personal Details Request Email Confirmation Template

Model Media Release Form

Document Retention & Disposal Procedure

Contents

Created: August 24
Review: August 25

Sarah Ludlow
Director of Quality

Introduction

Central Training Academy ("Central") is registered as a Data Controller under the Data Protection Act 2018, under the General Data Protection Regulation (GDPR).

Central needs to keep certain information about employees, learners, employers and other users to allow it to monitor performance, achievements, and other contractual or legal requirements. It is also necessary to process information so that staff can be recruited and remunerated, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Central must comply with the Data Protection Principles which are set out in the Data Protection Act 2018, the General Data Protection Regulation (hereafter referred to as the GDPR).

The Types of Information Covered by Data Protection Legislation

Personal Data

Data Protection legislation applies to personal information relating to a living person. It applies not only to computerised or automated personal data, but also to information held in manual filing systems. Included are such items of information as name, date of birth, contact details, title and gender, but also, less obviously, personal data such as IP addresses, online identifiers and pseudonyms. The legislation also applies to any records where an individual can be directly or indirectly identified from the information present, even where the name is not included.

Sensitive Personal Data

Also known as Special Category Data, this is the subset of Personal Data where the data items are especially sensitive and need a greater level of protection. These include ethnic origin, health data, religion, sexual orientation, and biometric information.

Central's Responsibilities

Under the Data Protection Act 2018 and the GDPR, the data protection principles set out the main responsibilities for Central. These require that data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing.

Central must have a lawful basis for processing any personal information and must make this clear in the Privacy Notice (Appendix 1).

The Data Controller and the designated Data Protection Officer

Central as a corporate body is the Data Controller under the Act and the Board is therefore ultimately responsible for compliance with the statutory legislative requirements. The Group Managing Director and Chairman takes this overall responsibility for compliance and delegates the overseeing of the implementation, giving advice and dealing with the subject access requests to the Data Protection Officer.

The Data and Funding Officer is the Data Protection Officer.

The Rights of Individuals Whose Data is Processed by the College

The right to be informed

The College is obliged to provide fair processing information and does so through its privacy notices.

The right of access

Individuals have the right to access their personal data, and this access will be provided as quickly as possible – we are legally bound to provide the data within one calendar month. This data will usually be provided free of charge, with the only exceptions being where the request is found to be unfounded, excessive or repetitive.

The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

The right to erasure

An individual is entitled to request the deletion or removal of personal data where there is no compelling reason for its continued processing. It should be noted that Central is legally obliged to process and retain much of the personal information it holds.

The right to restrict processing

Individuals have the right to restrict the College from processing certain aspects of their personal data if one of the following circumstances applies:

- The accuracy of the data is contested
- The individual objects to the processing of the data in principle
- Central's processing of the data is unlawful
- Central wishes to delete the data, but the individual has need of the data for legal purposes.

The right to data portability

Individuals may request an electronic copy of their personal data to use for their own purposes. Central will make every effort to provide the data in a form that is usable and acceptable to the individual, and this will be done without charge.

The right to object

Individuals have the right to object to:

- Direct marketing – Central will stop processing for this purpose on receipt of an objection.
- Data processing for research or statistics – Central will engage with the individual to come to an agreement within the law.
- Data processing in Central's legitimate interests - Central will engage with the individual to

come to an agreement within the law.

Rights in relation to automated decision making and profiling individuals who have any concerns about automated or computerised decision making should refer them to the Data Protection Officer.

The Responsibilities of Staff

- To ensure that any information that they provide to Central in connection with their employment is accurate and up to date.
- To inform Central of any change to the information which they have provided.
- To check the information that Central will send out from time to time, giving details of information kept and processed about staff, and change any information that is incorrect or incomplete.
- To comply with the guidelines for data collection and processing when, as part of their responsibilities, they collect information about other people, (for example learners' course work, opinions about ability, references to other academic institutions, or details of personal circumstances).

Responsibilities of Learners

- To ensure that all personal data provided to Central is accurate and up to date.
- To ensure that changes of address, next of kin etc. are notified to Central, preferably via their Course Tutor or the administration office.
- To ensure that they keep their passwords to Central networks and systems secret and secure.
- To report to their Course Tutor if they suspect their account security has been breached.

Data Security

In order to ensure the security of personal information, IT Services will:

- maintain a high level of security guarding Central's network and systems
- enforce encryption on portable devices
- prevent users from storing data on local drives of non-portable IT hardware
- wipe hard drives and memory of all equipment before disposal.

In order to ensure the security of personal information, staff are required to:

- lock their IT device using **[Ctrl]-[Alt]-[Delete]**, then **[Enter]** when leaving their PC /Laptop unattended
- keep their passwords secret
- avoid opening emails on a projected screen – private information may be displayed to anyone else in the room or even outside via the window
- when emailing personal data, password protect in an attachment and phone the password through to a trusted number
- refer all requests for disclosure of personal data from external sources to be dealt with via the administration office

- contact the Data Protection Officer if in doubt about any data security matter
- check the email addresses of intended recipients before sending any email, as email programs often incorrectly predict email addresses you are typing in
- consider using BCC to restrict visibility of other recipients' addresses when emailing to a group of recipients (especially where there are large numbers of recipients or some external addresses).

Where Central processes data on behalf of other organisations, e.g. conducting

external DBS checks, it will comply to ICO requirements.

Loss or Theft of Personal Information

All incidences of loss or theft of personal information must be reported immediately to Central's Data Protection Officer. A data or IT security incident relating to breaches of security and/or confidentiality could range from computer users sharing passwords, to the loss or theft of personal information either inside or outside Central.

A security incident is any event that has resulted, or could result in:

- The disclosure of personal/sensitive/confidential information to any unauthorised person.
- The integrity of the system or data being put at risk.
- Threat to personal safety or privacy.
- Legal obligation or penalty.

All incidents must be reported to the Data Protection Officer in the first instance, as soon as possible after the event.

In the case of a potential breach, the Data Protection Officer will instigate an investigation into the incident and will decide whether it needs to be reported to any regulatory bodies, in particular the Information Commissioner's Office (ICO). If a breach has occurred, the ICO will be informed within 72 hours of the incident, and if appropriate all data subjects concerned will also be contacted and informed. If possible, the offending paperwork, data or communication will be retrieved as soon as possible. The Data Protection Officer will retain a central register of all such incidents occurring within Central, whether or not they resulted in a breach.

The following is a list of examples of breaches of security and breaches of confidentiality. It is neither exclusive nor exhaustive and should be used as a guide only. If there is any doubt as to what constitutes an incident, you should consult the Data Protection Officer who will decide what action should be taken.

Examples of a breach of confidentiality:

- Finding confidential/personal information either in hard copy or on a portable media device outside Central premises or in any of Central's unsecured common areas.
- Finding any records about a staff member, learner, or applicant in any location outside the Central's premises.
- Passing information to unauthorised people either verbally, in writing or electronically.

Subject Consent

In many cases, Central can only process personal data with the consent of the Individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to Central processing some specified classes of personal data is a condition of acceptance of a learner onto any course, and a condition of employment for staff. This includes information about previous unspent criminal convictions (all convictions in the case of staff).

Therefore, all prospective staff and learners will be asked to sign a Privacy Notice, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

Where images and videos of learners or models are going to be used for promotional activities etc, then a Model Media Release Permission form must be obtained. (Appendix 3)

Personal Details Request Procedure

When sending learner's or members of staff's personal details via email, Central will ensure to use the following procedure.

Step 1: Check the email address and date of birth of the personal making the request over the phone.

Step 2: Inform the person making the request that we will send a confirmation request email.

Step 3: Send an email to the recipient asking them to reply to confirm that this is their email and confirm their full name and date of birth.

Step 4: Check that the details given in the confirmation email match those given over the phone.

Step 5: Keep copies of both emails in the learner's or member of staff's personal file.

An email template is provided for this purpose (Appendix 2). This template will be used at step 3 above.

Document Retention and Disposal

Any decision regarding retaining or disposing of a document(s) should be taken in accordance with the Document Retention and Disposal procedures (Appendix 4).

Conclusion

Compliance with the Data Protection Act 2018, the GDPR, is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to Central's facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of the policy should be taken up with the Data Protection Officer.

If you require any further information on the Data Protection Act 2018, the superseding General Data Protection Regulation, or how any aspect is implemented at Central Training Group please make contact with:

Data Protection Officer
44 Alexandra Street
Southend-On-Sea Essex
SS1 1BJ

Tel: 01702 671332

Email: DPO@centraltraininggroup.com

Useful Links:

Information Commissioner Office: www.ico.gov.uk

Related Documents:

Appendix 1: Privacy Notice
Appendix 2: Personal Details Request Form
Appendix 3: Model Media Release Form
Appendix 4: Document Retention & Disposal
Procedure HR & Staff Development Policy
Equality and Diversity Policy
Staff Handbook
Managers
Handbook Online
Safety Policy DBS
Vetting Policy
Safeguarding Policy

Appendix 1: Privacy Notice

This notice describes how Central Training Group uses and protects the personal information you provide to us.

Who does this apply to?

People who use or may use our services. This includes:

- Visitors to our website
- Individuals who study a course with us
- Employers who request training from us
- Employers who take learners on work experience
- Employers who employ an apprentice
- Individuals who request information from us
- Subcontractors

If you are asked to provide information to us, it will only be used in the ways described in our Data Protection Policy and Privacy Notice.

How we collect your information

We may collect your personal data in a number of ways, for example:

- From the information you provide to us when you interact with us before joining, for example when you express your interest in studying at Central Training Group.
- When you apply to study at Central Training Group and complete enrolment forms via the admissions processes and procedures.
- When you communicate with us by telephone, email or via our website or social media, for example in order to make enquiries or raise concerns.
- In various other ways as you interact with us during your time as a leaner of Central Training Group for the various purposes set out below.
- From third parties, for example from your previous or current school, sixth form college, FE college or university or employers who may provide a reference about you or who may sponsor your studies.

How we use your personal information

We may process your personal data because it is necessary for the performance of a contract with you or in order to take steps at your request prior to entering into a contract. In this respect, we will use your personal data for the following:

- To meet our legal and statutory duties and responsibilities
- To process applications and enrolments
- For our own internal records
- To contact you in response to an enquiry

- To contact you about the services we provide
- To be shared with other organisations for education, training & employment purposes, including the Education and Skills Funding Agency, OFSTED, Department for Education.
- To monitor and evaluate the performance and effectiveness of our programmes.
- To promote equality and diversity throughout our centres.
- To assess your eligibility for bursary payments
- To providing learning support
- Safeguarding
- For the prevention and detection of crime

We may also process your personal data where:

- It is necessary for medical purposes
- It is necessary to protect your or another person's vital interests
- We have your specific, or where necessary, explicit consent to do so

At no time will we assume your permission to use information that you provide for anything other than the reasons stated here.

The lawful basis on which we use this information

To conform with Article 6 and Article 9 of the General Data Protection Regulation, we collect and use your personal information under the lawful basis of meeting our contractual obligation with the Education and Skills Funding Agency for the purposes of claiming public money to fund your training programme.

The categories of learner information that we collect include:

- Personal information (such as name, unique learner number and address)
- Identity details (such as passport number, settled status, leave to remain)
- Characteristics (such as ethnicity, gender, language, nationality, country of birth)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Website usage data
- Information relating to your education and employment history
- Sensitive personal data and information about criminal convictions and offences
- Special Educational Needs information
- Financial information (such as bank details)
- Behavioural information
- Relevant medical information
- CCTV images on college premises

Collecting learner information

Whilst the majority of learner information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain learner information to us or if you have a choice in this.

Links From Our Site

Our website may contain links to other websites. Please note that we have no control of websites outside of www.centraltraininggroup.com if you provide information to a website to which we link, we are not responsible for its protection and privacy. You are advised to read the privacy policy or statement of other websites prior to using them.

People who use our services

We hold the details you provide us with in order to deliver programmes of study, including Apprenticeships, Educational programmes for younger people, and other services which meet your specific needs.

We only use these details to provide the service you have requested and for other closely related purposes. For example, we might use information about people who have enquired about a course to carry out a survey to find out if they are happy with the level of service they have received.

You are able to request that we stop contacting you at any time.

People who use our commercial services

If you are a customer of a commercial service of Central e.g. Hairdressing and Barbering Centres, the information you provide us with to enable us to deliver that service will only be held and used for that purpose or for other closely related purposes e.g. we might use information about people who use the Hair Salons to send out offers about the services.

People who request information from us

If you request information from us by letter, telephone, email, submitting an enquiry on the website or from a sales appointment, we will make a record of that enquiry and will use the information you give us to provide you with a response. We will only use the information for these purposes and to provide a follow up service to ensure that we provided you with what you asked for.

You are able to request that we stop contacting you at any time.

Any emails sent to us, including attachments, may be monitored. Please be aware that you have a responsibility to ensure that any email you send us is in the bounds of the law.

Security

We will hold your information securely.

To prevent unauthorised disclosure or access to your information, we have implemented strong organisational and technical security safeguards.

Storing learner data

We will hold your personal information in paper and electronic form. Your data will be securely destroyed as listed below. We will ensure that all personal information supplied is held securely in accordance with the Data Protection Act 2018.

We keep your personal data for:

Status	Held for
Course applicant	6 months
Learner (started a programme)	7 years from leaving date

Who we share learner information with

We routinely share learner information with:

- the Education and Skills Funding Agency (ESFA)
- the Department for Education (DfE)
- Local Authorities
- Awarding Organisations
- the Police
- Other bodies if required by the law
- Parents and Guardians (for those aged 16-18 or 19-24 if you are a vulnerable adult)
- for the prevention and detection of crime.

Why we share learner information

We do not share information about our learners with anyone without consent unless the law and our policies allow us to do so.

We share learners' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins college funding and educational attainment policy and monitoring.

Your information may by necessity be disclosed to appropriate staff members of Central Training Group.

We will only share your personal information with other people (parents, carers or with agencies such as the DWP, with your permission).

Data collection requirements

To find out more about what learner personal data is collected by the Department for Education, through the Education and Skills Funding Agency, and how it is handled visit https://www.gov.uk/government/publications/esfa-privacy-notice

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and learners have the right to request access to information about them that we hold and to have any inaccuracies corrected. To make a request for your personal information, or be given access to your child's educational record, contact:

Data Protection Officer DPO@centraltraininggroup.com

If you request information, we aim to provide this to you, where possible, within 30 days. Where this is not possible, we will keep you informed.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress.
- Prevent processing for the purpose of direct marketing.
- Object to decisions being taken by automated means.
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Controlling Information About You

When you fill in a form or provide your details on our website, you may see one or more tick boxes allowing you to:

• opt in to receive marketing communications from us by e-mail, telephone, text message or post

• opt in to receive marketing from our sponsors, third party partners by e-mail telephone, text message or post.

If you have agreed that we can use your information for marketing purposes, you can change your mind easily, via one of these methods:

• send an e-mail: DPO@centraltraininggroup.com

• write to:

DPO

Central Training Group 44
Alexandra Street
Southend-On-Sea Essex
SS1 1BU

Changes to This Privacy Notice

We will keep this Privacy Notice under regular review and reserve the right to change it as necessary from time-to-time or if required by law. Any changes will be immediately posted on the website.

Contact

If you would like to discuss anything in this privacy notice, please contact: Data

Protection Officer

DPO@centraltraininggroup.com

Appendix 2: Personal Details Request Email Confirmation Template

Dear ……..

Thank you for your request in respect of:

……

In order for us to confirm the details you require please reply to this email to confirm this is your email address and provide the details below:

YOUR FULL NAME

YOUR DATE OF BIRTH

As soon as we have received your confirmation email, we will send you the information you requested.

Kind regards

It is recommended that you copy and paste this into a blank email in Outlook then save as a template in *your* draft folder. This will ensure easy access as and *when* you need to use it

Appendix 3: Model Media Release Form

Central Training Group Model Media Release Permission
(Learners and Clients)

Name of Client:		**Age** (if under 18)	
Name of Learner:			
Location of service:			

I confirm that I give permission for the image/video of my hairdressing service to be used:

- To promote hairdressing courses on social media channels by photograph and/or videos.
- On publications about the hairdressing programmes offered by Central.
- Within the Central Training Magazine.
- On flyers to be distributed to the public.
- On posters within centres.
- On the Central Training Group website.
- Within a learner collection of learning evidence.

Privacy Notice

Central Training Group is a registered Data Controller and is subject to the Data Protection Act 2018 and the General Data Protection Regulations. Please read our Privacy Notice (on following pages) and Data Protection Policy to see how we use and protect your personal data http://www.centraltraininggroup.com/contact

Client Signature:	
Learner Signature:	
Date:	

Links From Our Site

Our website may contain links to other websites. Please note that we have no control of websites outside of www.centraltraininggroup.com if you provide information to a website to which we link, we are not responsible for its protection and privacy. You are advised to read the privacy policy or statement of other websites prior to using them.

People who use our commercial services

If you are a customer of a commercial service of the College e.g. Hairdressing and Barbering Colleges, the information you provide us with to enable us to deliver that service will only be held and used for that purpose or for other closely related purposes e.g., we might use information about people who use the Hair Salons to send out offers about the services.

Security

We will hold your information securely.

To prevent unauthorised disclosure or access to your information, we have implemented strong organisational and technical security safeguards.

Appendix 4: Document Retention & Disposal Procedure

CONTENTS

Introduction

In the course of carrying out its various functions and activities, Central Training Group collects from individuals and external organisations and generates a wide range of data and information, which is recorded in documents. Many of these documents are subsequently retained in one form or another, e.g. as 'hard' paper records or on a computer system in digital form. For the avoidance of doubt the terms 'document' and 'records' should be taken to include documents/records which are in digital format.

Retention of specific documents may be necessary for one or more of the following reasons:

- To fulfill statutory or other regulatory requirements.
- To meet contractual funding agreements.
- To evidence events/agreements in the case of dispute(s).
- To meet operational needs.
- To ensure the preservation of documents of historic or other value.

However, the permanent retention of all documents is undesirable and to be discouraged. Disposal, where appropriate, is to be encouraged for the following reasons:

- There is a shortage of storage space.
- Retention of personal data which is no longer necessary may be unlawful.
- Reduction of fire risk (in the case of paper records).
- De-cluttering of office accommodation.
- Reduction of burden of Document Management as required by Freedom of Information Act 2000.

Scope and Purpose

The purpose of this Policy is to provide a corporate policy framework to govern decisions on whether, in any given case, a particular document (or set of documents) should be retained, and if so, in what format and for what period.

Retention and Disposal Policy

Any decision regarding retaining or disposing of a document should be taken in accordance with the retention/disposal policy. This policy consists of:

- The **key disposal/retention considerations** criteria checklist set out in Appendix 1 – essentially, no document should be disposed of unless all these have been considered in relation to the document.

- The **Retention Schedules** contained in Appendix 2. These provide guidance on recommended and mandatory minimum retention periods for specific classes of documents/records, where special rules/considerations apply.

Where a retention period has expired in relation to a particular document a review should always be carried out before a final decision is made to dispose of that document. Such reviews need not necessarily be detailed or time consuming. In the event that a decision is taken to dispose of

a particular document or set of documents, regard should be made to the method of disposal; and the disposal should be documented.

Roles and Responsibilities

Responsibility for determining (in accordance with the Retention/Disposal policy mentioned above) whether to retain or dispose of specific documents, rests with the Group Managing Director in respect of those documents that properly fall within the remit or control of their Service, but they may wish to appoint someone else to carry out this task. They should ensure, however, that any such person is fully conversant with this Policy and is also familiar with the operational requirements of the service so that they are able to assess the significance of documents.

Directors are expected to be proactive in carrying out or instigating audits of existing documentation that may be suitable for disposal. They are also expected to seek legal advice on whether minimum retention periods are prescribed by law, and whether retention is necessary to protect the company's position where the likelihood of a claim has been identified. External legal services cannot be expected to possess the operational or background knowledge required to assess whether, for example, a particular document may be required by the company concerned for operational needs arising in the future, or contains information that, if deleted, could cause embarrassment to Central Training. Again, it is the board of directors who are best placed to make such assessment.

Disposal

Disposal can be achieved by a range of processes:

- Binning
- Recycling
- Treatment as Confidential Waste
- Physical destruction on site (paper records) • Deletion – where computer files are concerned
- Transfer of document to external body.

In the selection of the method of disposal regard should be made to the considerations discussed below. Under no circumstances should paper documents containing personal data or confidential information be simply binned or sent for recycling without being shredded. To do so could result in the unauthorised disclosure of such information to third parties and render Central Training Group liable to prosecution or other enforcement action under the Data Protection Act 2018 and General Data Protection Regulation (GDPR), and also to serious embarrassment.

Documenting Disposal

Disposal should be documented – that is to say, a record should be kept detailing the document disposed of, the method, the date, and the director who authorised disposal. In particular, the record should be able to demonstrate that the disposal was in accordance with this policy or set out the (very exceptional) reasons for departing from it.

Data Protection Act 2018 and GDPR

Under the Data Protection Act 2018 and General Data Protection Regulation (GDPR) "personal data" processed for any purpose or purposes must not be kept for longer than is necessary for that purpose / those purposes.