The Adult Training Network GDPR Action Plan

- All staff and tutors are given the GDPR Q&A (see appendix 1) and can refer to https://www.eugdpr.org/gdpr-faqs.html for more information when learners ask for GDPR related questions.
- Enrolment forms changed to include GDPR privacy notice.
- ATN to carry out a data audit by filling in audit form (see appendix 2).
- ATN staff and tutors to complete online implementing GDPR training- https://www.e-learningwmb.com/blog/general-data-protection-regulation-free-e-learning
- Data breach form (see appendix 3) must be filled in within 72 hours of first becoming aware of the breach. This then must be passed onto ATN data protection officer who will respond accordingly.
- "Variation to terms and conditions" (see appendix 4) to be given to all staff who must read and confirm that they have understood.
- Staff and tutors to be given privacy notice for employees (see appendix 5).
- ATN to carry out data protection self-assessment- https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/
- Data subjects can make a subject access request to find out what data is being held, they can use the template (see appendix 6).

Appendix 1

Data protection – Q&A sheet

1. ***Why do you need all this data?***

We are legally obliged to collect this data for our contract with the Education and Skills Funding Agency, for Ofsted requirements and under the Equality and Diversity Act.
For the ESFA, ATN and their subcontractors have to add data to the ILR every month. The ILR stands for Individualised Learning Record, and each learning provider inputs the learner data to a central system. The ILR is an ongoing collection of data about learners and the learning they have done with any learning provider in the Further Education and Skills sector. If we cannot upload the information, we are not funded for your learning and therefore we cannot provide this course for free/for a subsidised amount.
The data is used for calculating funding and to evaluate the service provided.
Most of the data is collected under the obligations mentioned above. Some is still optional. This is made clear on your enrolment form *

2. ***Why is the enrolment form split into 2 sections? What is the difference?****

The majority of the information we collect is asked for because we have a legal obligation to fulfil our contract with our funders. Data that is collected is used to analyse what learning is taking place and where, and to see what has the most impact for our diverse population. The other section is where we would like to collect extra data to 'add more to this picture', to help us evaluate our service in more depth.

3. ***Can you explain 'legally obliged'? Why do the government need all this?***

When ATN run a contract on behalf of a funding body, we have to prove who we are funding, by enrolling learners on our system.

The ESFA and Department for Education use the data to:

- Determine **funding and commissioning decisions**
- **Inform the work of Ofsted** and other agencies
- Present the **progress and position** of the sector
- Inform **policy making** decisions
- Calculate **funding earned** by providers
- Enable **comparison** of actual volumes and costs against contracted levels.

For example, we are monitored by other agencies such as Ofsted. When we write reports on our provision, we use data that it is anonymous –we do not use names, we just present a picture i.e. xx% of our learners are male, or xx% of our learners are over 65. Ofsted look at our achievement rates and might ask why one group is not doing as well as another group. This also links to Equality and Diversity which Ofsted look at too – are we offering opportunities to all and are we offering support to those who need it?

4. ***I have the 'right to be forgotten'. Please can you delete all my data?***

Under our funding body rules, we are legally obliged to keep the data for a number of year, for example it is 7 years for ESFA funded courses. We cannot delete certain data until the end of that period. Under our policies and procedures we have mechanisms in place to ensure that we delete the right data at the right time.

5. How can I get hold of all the information you hold on me?

You have to raise a Subject Access Request (SAR) with your learning provider, and they will need to work with ATN to action this. (For DD staff, this request would come straight to Sarjeet Singh Gill).

A Subject Access Request has to be responded to without delay and at the latest within a month. If the request is especially complex, this may be extended. There is no fee for this, unless it is deemed that the request is unfounded or excessive, where an administrative cost could be applied.

6. How do I know you don't share my details?

We will not share your data outside of this without your consent, because this would be a breach of data protection law, unless specific conditions are met i.e. it is in the interests of health and safety (safeguarding).

ATN takes your data privacy very seriously. We will only share your information with a third party where it is necessary for providing this learning opportunity to you. For example, we have to enter your data onto a management information system called 'Learnertrack'. The provider of this system has signed an agreement with us saying that they will not share your data. We will keep your data secure. After the course ends, we will only use your contact details to contact you about progression, which is a requirement of our funding.

Your information will be securely destroyed after it is no longer required under agreed regulations from the funding body.

Further information about use of and access to your personal data; details of organisations with whom we share data; information about how long we retain your data; and how to change your consent to being contacted, please contact ATN on 020 8574 9588/020 8574 0795 or email sgill@adult-training.org.uk

Appendix 2

HR Data Audit Form

Category of personal data: *(FOR EXAMPLE, DISCIPLINARY RECORDS)*	
What is the purpose for processing the data?	
What category of person does the data relate to?	*Note: for example, this could be a prospective employee/employee/employee's family member]*
What is the source of the data?	
What date was the data collected?	
Where is the data stored?	
Is it live data or archived?	
How long is the data retained for?	
Was a privacy notice issued?	
Does a privacy notice need to be re-issued?	
Has the employee been made aware of their rights in relation to this data ie erasure, rectification, restriction, objection?	
Does the data fall into the "special categories" definition?	
Does the data relate to criminal convictions?	
Does the data involve automated decision making? If so, what decisions are made and what are the consequences will the decisions have on individuals?	

Who is responsible for ensuring accuracy of data?	
Who has access to the data?	
Are security controls in place to restrict access to this data? What are they?	
Is the data shared with anyone outside of the organisation? If so, who?	
Is the data shared with anyone outside of the EEA? If so, which countries is the data transferred to?	
How is the data destroyed when it is at the end of the retention period?	
What current policies apply to the data in question?	
Are these policies up to date?	
Which of the lawful bases for processing the data applies?	
If data is 'special' category, which of the lawful bases for processing the data applies?	

Appendix 3

Data Protection Breach report

Please complete this form and send to your line manager, with a copy to the ATN Data Protection Lead, Sarjeet Singh Gill at sgill@adult-training.org.uk

If Sarjeet Singh Gill is not available, please email Kamaljit Kaur at kamaljit@adult-training.org.uk

Date of incident	
Date of incident report	
Summary of the incident and action taken so far What happened? What data did this involve? What are the risks? Who else is involved? Who have you informed? What do you think we need to do immediately?	
Any action taken by you:	
Reported by (Name & Job title): Contact Number: x Report Date:	Signature (electronic if possible):

Appendix 4

Variation to terms and conditions

Important information about changes to your current employment documentation due to the introduction of new data protection laws

The General Data Protection Regulation (GDPR) will come into force in the UK on 25th May 2018 through a new Data Protection Act. We are committed to the principles of data security outlined in the GDPR and ensuring our compliance with our data protection obligations.

We have set out below some changes that are required because of the new laws, including a set of new policies that will come into effect on 25th May 2018.

Changes to your employment documentation

We have reviewed our current position in relation to GDPR and have identified new policies which are needed or which must replace existing ones. This law, and the UK's own new Data Protection Act, will replace current data protection laws. Therefore, any references to the Data Protection Act 1998 in your current contractual documentation are, by way of this document, replaced with a reference to the General Data Protection Regulation and the Data Protection Act in force from time to time.

Our new policies are set out below and will come into effect from 25th May 2018:

- Data protection policy
- Communications policy
- Policy on your rights in relation to your data
- Data breach notification policy
- Subject access request policy

We have also implemented new privacy notices to be effective from 25th May 2018, which set out what personal data we use and how we use it:

- Privacy notice for employees
- Privacy notice for job applicants

Changes to your current Employee Handbook/Statement of Main Terms of Employment

1. The following clause in your employee handbook, 'DATA PROTECTION ACT 1998' is, with effect from 25th May 2018, replaced with:

DATA PROTECTION

The General Data Protection Regulation (GDPR) and the current Data Protection Act regulate our use of your personal data. As an employer it is our responsibility to ensure that the personal data we process in relation to you is done so in accordance with the required principles. Any data held shall be processed fairly and lawfully and in accordance with the rights of data subjects.

We will process data in line with our privacy notices in relation to both job applicants and employees.

You have several rights in relation to your data. More information about these rights is available in our "Policy on your rights in relation to your data". We commit to ensuring that your rights are upheld in accordance with the law and have appropriate mechanisms for dealing with such.

We may ask for your consent for processing certain types of personal data. In these circumstances, you will be fully informed as to the personal data we wish to process and the reason for the processing. You may choose to provide or withhold your consent. Once consent is provided, you are able to withdraw consent at any time.

You are required to comply with all company policies and procedures in relation to processing data. Failure to do so may result in disciplinary action up to and including dismissal.

2. The following clause in your employee handbook, 'THIRD PARTY INVOLVEMENT' is, with effect from 25th May 2018, replaced with:

THIRD PARTY INVOLVEMENT

We reserve the right to allow third parties to chair any meeting, for example disciplinary, capability, grievance, this is not an exhaustive list. We will seek your consent at the relevant time to share relevant 'special categories of data' where it is necessary for the purposes of that hearing.

3. The following clauses in your employee handbook, 'DISCLOSURE AND BARRING CERTIFICATES', and 'POLICY STATEMENT ON THE SECURE STORAGE, HANDLING, USE, RETENTION AND DISPOSAL OF DISCLOSURES AND DISCLOSURE INFORMATION' are, with effect from 25th May 2018, replaced with:

DISCLOSURE AND BARRING CERTIFICATE(S)

Your initial employment is conditional upon the provision of a satisfactory Disclosure and Barring Certificate of a level appropriate to your post. You may be required to undertake to subsequent criminal record checks from time to time during your employment as deemed appropriate by the Company. In the event that such certificate(s) are not supplied your employment with us will be terminated.

POLICY STATEMENT ON THE SECURE STORAGE, HANDLING, USE, RETENTION AND DISPOSAL OF DISCLOSURES AND DISCLOSURE INFORMATION

During your employment, you are required to immediately report to the Company any convictions or offences with which you are charged, including traffic offences.

1) As an organisation using the Disclosure and Barring Service and/or Disclosure Scotland to help assess the suitability of applicants for positions of trust, we comply fully with the Disclosure and Barring Service/Disclosure Scotland Code of Practice regarding the correct handling, use, storage, retention and disposal of disclosures and disclosure information. We also comply fully with our obligations under the Data Protection Act.

2) Disclosure information is never kept in an applicant's personnel file. It is always kept separately and securely in lockable, non-portable storage containers with access strictly controlled and limited to those who are authorised to see it as part of their duties in accordance with Section 124 of the Police Act 1997.

3) We maintain a record of all those to whom disclosures and disclosure information has been revealed and we recognise that it is a criminal offence to pass the information to anyone who is not entitled to

receive it.

4) Disclosure information is only used for the specific purpose for which it was requested.

5) Once a recruitment (or other relevant) decision has been made, we do not keep disclosure information for any longer than is absolutely necessary in order to allow for the consideration and resolution of any disputes or complaints. Where appropriate, the Disclosure and Barring Service/Disclosure Scotland will be consulted and full consideration will be given to the data protection and human rights of the individual.

6) Once the retention period has elapsed, we will ensure that any disclosure information is immediately destroyed by secure means, i.e. by shredding, pulping or burning. While awaiting destruction, disclosure information will not be kept in any insecure receptacle (e.g. a waste bin or confidential waste sack). We will not keep any photocopy or other image of the disclosure or any copy or representation of the contents of the disclosure. However, we may keep a record of the date of issue of the disclosure, the name of the subject, the type of disclosure requested, the post for which the disclosure was requested, the unique reference number of the disclosure and the details of the recruitment (or other relevant) decision taken.

4. The clause entitled 'Monitoring' in the Email and Internet Policy is, with effect from 25th May 2018, amended as follows:

We reserve the right to monitor all e-mail/internet activity by you for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements. This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are subject to the same rules as your work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

5. Any reference to the term "sensitive data" contained in your employment documentation is, with effect from 25th May 2018, replaced with "special categories of data".

Appendix 5

PRIVACY NOTICE FOR EMPLOYEES/WORKERS

In accordance with the General Data Protection Regulation (GDPR), we have implemented this privacy notice to inform you, our employees, of the types of data we process about you. We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

This notice applies to current and former employees and workers.

A) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing is fair, lawful and transparent
b) data is collected for specific, explicit, and legitimate purposes
c) data collected is adequate, relevant and limited to what is necessary for the purposes of processing
d) data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) we comply with the relevant GDPR procedures for international transferring of personal data

B) TYPES OF DATA HELD

We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data, as appropriate to your status:

a) personal details such as name, address, phone numbers
b) name and contact details of your next of kin
c) your photograph
d) your gender, marital status, information of any disability you have or other medical information
e) right to work documentation
f) information on your race and religion for equality monitoring purposes
g) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter
h) references from former employers
i) details on your education and employment history etc
j) National Insurance numbers
k) bank account details
l) tax codes
m) driving licence
n) criminal convictions

o) information relating to your employment with us, including:

   i) job title and job descriptions
   ii) your salary
   iii) your wider terms and conditions of employment
   iv) details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
   v) internal and external training modules undertaken
   vi) information on time off from work including sickness absence, family related leave etc

p) CCTV footage
q) building access card records
r) IT equipment use including telephones and internet access.

C) COLLECTING YOUR DATA

You provide several pieces of data to us directly during the recruitment period and subsequently upon the start of your employment.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

Personal data is kept in files or within the Company's HR and IT systems.

D) LAWFUL BASIS FOR PROCESSING

The law on data protection allows us to process your data for certain reasons only. In the main, we process your data in order to comply with a legal requirement or in order to effectively manage the employment contract we have with you, including ensuring you are paid correctly.

The information below categorises the types of data processing, appropriate to your status, we undertake and the lawful basis we rely on.

Activity requiring your data	**Lawful basis**
Carry out the employment contract that we have entered into with you e.g. using your name, contact details, education history, information on any disciplinary, grievance procedures involving you	Performance of the contract
Ensuring you are paid	Performance of the contract
Ensuring tax and National Insurance is paid	Legal obligation
Carrying out checks in relation to your right to work in the UK	Legal obligation
Making reasonable adjustments for disabled employees	Legal obligation
Making recruitment decisions in relation to both initial and subsequent employment e.g. promotion	Our legitimate interests
Making decisions about salary and other benefits	Our legitimate interests
Ensuring efficient administration of contractual benefits to you	Our legitimate interests
Effectively monitoring both your conduct, including timekeeping and attendance, and your performance and to undertake procedures where necessary	Our legitimate interests
Maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and	Our legitimate interests

appropriate contact points in the event of an emergency are maintained	
Implementing grievance procedures	Our legitimate interests
Assessing training needs	Our legitimate interests
Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments	Our legitimate interests
Gaining expert medical opinion when making decisions about your fitness for work	Our legitimate interests
Managing statutory leave and pay systems such as maternity leave and pay etc	Our legitimate interests
Business planning and restructuring exercises	Our legitimate interests
Dealing with legal claims made against us	Our legitimate interests
Preventing fraud	Our legitimate interests
Ensuring our administrative and IT systems are secure and robust against unauthorised access	Our legitimate interests
Providing employment references to prospective employers, when our name has been put forward by the employee/ex-employee, to assist with their effective recruitment decisions	Legitimate interest of the prospective employer

E) SPECIAL CATEGORIES OF DATA

Special categories of data are data relating to your:

a) health
b) sex life
c) sexual orientation
d) race
e) ethnic origin
f) political opinion
g) religion
h) trade union membership
i) genetic and biometric data.

We carry out processing activities using special category data:

a) for the purposes of equal opportunities monitoring
b) in our sickness absence management procedures
c) to determine reasonable adjustments

Most commonly, we will process special categories of data when the following applies:

a) you have given explicit consent to the processing
b) we must process the data in order to carry out our legal obligations
c) we must process data for reasons of substantial public interest
d) you have already made the data public.

F) FAILURE TO PROVIDE DATA

Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract of employment with you. This could include being unable to offer you employment, or administer contractual benefits.

G) CRIMINAL CONVICTION DATA

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment. We use criminal conviction data to determine your suitability, or your continued suitability for the role. We rely on the lawful basis of our legitimate interests to process this data.

H) WHO WE SHARE YOUR DATA WITH

Employees within our company who have responsibility for recruitment, administration of payment and contractual benefits and the carrying out performance related procedures will have access to your data which is relevant to their function. All employees with such responsibility have been trained in ensuring data is processing in line with GDPR.

Data is shared with third parties for the following reasons: for the administration of payroll and for Disclosure Barring Service (DBS) checks.

We may also share your data with third parties as part of legal obligations. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

We do not share your data with bodies outside of the European Economic Area.

I) PROTECTING YOUR DATA

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such.

J) RETENTION PERIODS

We only keep your data for as long as we need it for, which will be at least for the duration of your employment with us though in some cases we will keep your data for a period after your employment has ended. Some data retention periods are set by the law. Our retention periods are: Retention periods can vary depending on why we need your data, as set out below: please refer to the ATN retention policy which can be found at http://www.adult-training.org.uk/policies.html.

K) AUTOMATED DECISION MAKING

Automated decision making means making decision about you using no human involvement e.g. using computerised filtering equipment. No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

L) EMPLOYEE RIGHTS

You have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;
b) the right of access to the data we hold on you. More information on this can be found in our separate policy on Subject Access Requests;
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
g) the right to object to the inclusion of any information;
h) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on employee rights under GDPR.

M) CONSENT

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

N) MAKING A COMPLAINT

If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

O) DATA PROTECTION COMPLIANCE

Our Data Protection Officer is:

Sarjeet Singh Gill
sgill@adult-training.org.uk
020 8574 0795 / 020 8574 9588

Appendix 6

Letter template

[Your full address]

[Phone number]

[The date]

[Name and address of the organisation]

Dear Sir or Madam

Subject access request

[Your full name and address and any other details to help identify you and the data you want.]

Please supply the data about me that I am entitled to under data protection law relating to: [give specific details of the data you want, for example:

- my personnel file
- CCTV camera situated at ('location E') on 23 May 2017 between 11am and 5pm
- copies of statements (between 2013 and 2017) held in account number xxxxx.]

If you need any more data from me, or a fee, please let me know as soon as possible. It may be helpful for you to know that data protection law requires you to respond to a request for data within one calendar month.

If you do not normally deal with these requests, please pass this letter to your DataProtection Officer, or relevant staff member. If you need advice on dealing with this request, the Information Commissioner's Office can assist you. Its website is ico.org.uk or it can be contacted on 0303 123 1113.

Yours faithfully

[Signature]