DATA PROTECTION AND INFORMATION SECURITY POLICY

Introduction

Under the Data Protection Act and with GDPR (General Data Protection Regulation 2016), Creative Alliance is fully accountable for the ways in which the company keeps and uses personal data.

This policy explains the types of data Creative Alliance may hold, in both manual and computerised formats, relating to all employees (permanent full-time, hourly, fixed term contract, permanent part-time and freelance), regardless of seniority and any third-party service provider in contact with our users.

As an organisation that collects, uses and stores Personal Data Creative Alliance recognises that having controls around the collection, use, retention and destruction of Personal Data is important to comply with the Creative Alliance's obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

Creative Alliance has implemented this Data Protection Policy to ensure all Creative Alliance staff are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in Creative Alliance and will provide for a successful working and learning environment for all.

Creative Alliance Staff

All Creative Alliance staff have a responsibility to ensure all company personal data is securely maintained and correct processes are followed. Data protection is more than just protecting data from unauthorised access: it's about ensuring it is used for the sole purpose it was collected and respecting the privacy of the individual's data.

All staff will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This policy does not form part of any member of the Creative Alliance staff's contract of employment and Creative Alliance reserves the right to change this Policy at any time. All members of Creative Alliance staff are obliged to comply with this Policy at all times.

Why we collect Data

Creative Alliance collects, holds and manages data about individuals and organisations. We do this to provide a service to each person and organisation. We recognise our fundamental need to ensure that this information is accurate and secure.

This policy ensures Creative Alliance and its partners:
- comply with all data protection legislation (GDPR and DPA 1998) and follow the good practice set out by the Information Commissioner (ICO)
- Protect the rights of customers, partners and staff
- Are open about how it collects, stores, manages, processes and protects individuals' and organisations' data
- Protect themselves from the risks of a data breach

213 Scott House,
Custard Factory, Gibb Street,
Digbeth, Birmingham, B9 4AA

0121 753 0049
info@creativealliance.org.uk
www.creativealliance.org.uk

About This Policy

This Policy (and the other policies and documents referred to in it) sets out the basis on which Creative Alliance will collect and use Personal Data, It applies to all Personal Data stored electronically, in paper form, or otherwise.

If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring Creative Alliance's compliance with this Policy.

Creative Alliance will process data for a number of reasons including the following:

- Delivery of services to pupils.
- Recruitment and employment purposes.
- Completion of statutory returns.
- Health and Safety and occupational health of employees.
- Discipline and Grievance.
- Training and Development.
- Equal Opportunities.
- Criminal Offences.
- Information Sharing Protocols/Procedures (See Appendix 2 and 3).

This data will be kept for all current employees, volunteers, sessional workers service users and former employees and former volunteers, former sessional workers and former service users, pupils for a period of time to meet the legal obligations and/or operational reference, thereafter, the data will be destroyed in accordance with Creative Alliance Data Protection officer (DP0) who is the Operations Manager, John Parker.

Data may also be kept on contractors and visitors and agency workers permitted by the Act.

Creative Alliance Staff General Obligations

- Creative Alliance staff must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.
- Creative Alliance staff must not release or disclose any Personal Data: outside Creative Alliance; or inside Creative Alliance to Creative Alliance staff not authorised to access the Personal Data, without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

DATA PROTECTION PRINCIPLES

When using Personal Data, Data Protection Laws require that Creative Alliance complies with the following principles. These principles require Personal Data to be:

- processed lawfully, fairly and in a transparent manner;
- 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 for the purposes for which it is being processed;
- accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;

- kept for no longer than is necessary for the purposes for which it is being processed; and processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Responsibilities
The DPC's role is to monitor the Data Recording to ensure it meets the requirements of the Act and to report any violations to the Director, Noel Dunne. The DPC will keep records of all requests for information under the Data Protection Policy and the decision made in response to every request.

The Director will make employees/volunteers aware of their responsibilities in relation to Data Protection in their area of work during their induction period. It then becomes the employee's responsibility to ensure what should be kept or destroyed. If in doubt they should ask the DPC.

The DPC must also ensure that data recorded meets the General Principles of the Act. Personal or sensitive data must:

1. Be processed fairly and lawfully and may not be processed unless the information and consent requirements have been met.
2. Be obtained for specified and lawful purposes and must not be processed in any manner incompatible with those purposes.
3. Be adequate, relevant and not excessive for those purposes.
4. Be accurate and where necessary be up to date.
5. Be kept no longer than necessary for those purposes.
6. Be processed in accordance with individual rights.
7. Be safeguarded from unauthorised or unlawful processing and from accidental loss, destruction or damage.
8. Not be transferred to a country outside of the EU without adequate data protection arrangements.

Management
To comply with the Policy and only obtain, store, use or disclose data in accordance with the Policy, management must also assist the DPC and the individual concerned where this is required. Management should attend relevant training in order to understand their duties under the policy.

Other Employees/Volunteers
To obey this Policy and not store or disclose any personal information/data without the permission of the DPC and the individual concerned where this is required.

Lawful use of Personal Data
These are set out in Article 6 of the GDPR and are as follows:
- the use of the Personal Data is for the purposes of the legitimate interests of the Controller;
- the processing is necessary for the performance of a contract;
- the processing is necessary for compliance with a legal obligation;
- the processing is necessary in order to protect the vital interests of the individual or of another natural person;
- the processing is necessary for the performance of a task carried out in the public interest; and the individual who is the subject of the Personal Data has given consent for one or more specific purposes.

Raising Concerns/ Access to One's Personal Data

Members of staff who have concerns or wish to see personal data should raise the issue in the first instance with the Director. Service users/former service users must raise their request with the DPC. These requests should be communicated to the DPC and information must be supplied within 40 days of the request. There will be few exceptions when data will be confidential and will not be available for the individual to review. However, data will not be made available to a third party, unless there is a legal obligation, a genuine occupational requirement within the law, or without the employees/volunteers/sessional workers or service users/former service users permission.

For all records there will be a fee of £10 charged to supply information/access to records. All requests for data from the individual or from a third party must recorded and passed to the DPC even if this information request is denied.

Types of Data

- Service users' records, eg Individual Support Plans etc.
- Data related to child protection issues.
- Data related to employment of staff, (i.e. interview notes, CVs, application forms, tests, qualifications).
- Contractual documentation.
- Training records.
- Appraisals, development reviews.
- Enrolling learners onto training programmes
- Holding data for employers and learners for ESFA contract requirements.
- Holding data for learners and employers for the reporting of data and quality of our apprenticeship programme.
- Documents relating to an individual to provide training services
- Any other data required for the individual service
- Tracking of learner and employer's information in relation to tracking our success rates and impact of the training we deliver after the apprenticeship has finished
- References received and given by Creative Alliance, including credit references.
- Records concerning disciplinary and grievance and capability investigations and proceedings.
- Transfer, promotion or redeployment records.
- Absence records including annual leave, self-certification and medical forms.
- Accidents and occupational health and safety matters.
- Accounts/Budgets/Bank Accounts/Audits/Payroll related information.
- Volunteer Records etc.

All computerised data included in the above. Access will only be available to the Director.
All computerised systems will be password protected and have access rights, therefore only allowing access to authorised personnel. Other electronic systems, available for company use, which may be used for company use are:

- Email.
- Internet.
- Telephones.
- CCTV Systems.
- Server log-on if it identifies where individuals are located or when they are accessing their system.
- Other work monitoring or measurement systems.

This list is not exhaustive.

Archiving Procedure
Personal information must not be kept for longer than necessary. Retention periods are outlined and attached in Appendix 1. All archiving will carry a notification date for destroying in line with the retention period indicated on the list.

Every year the archiving of notes will be assessed by John Parker. The documentation will be stored in the archiving storage. Documents which are destroyed, will be shredded or placed in confidential bags in readiness for confidential shredding.

Information held electronically which is out of date yet needs to be retained for a further 3 years will not be permanently deleted but put into safe archive 'off line' folder.

Data handling
Child information obtained must only be used for legitimate professional reasons associated with purposes set out in the Children Act 2004 regulations. Information must not be accessed on behalf of a third party unless already authorised in guidance.

Child information obtained must not be retained for longer than necessary.

Child information obtained must be secured to prevent unauthorised disclosure (for example, not left unattended on desk). This information can be shared in line with the HM Government information sharing guidance.

APPENDIX 1 - RETENTION OF DOCUMENTATION

The Data Protection Act (DPA) applies to most types of records, whether held in paper, microform, or computerised format. Computerised systems are covered by the law, as are certain manual systems: to be covered, manual systems must be organised into a 'relevant filing system'.

Subject to certain exceptions (as detailed in Schedule 7 of the Data Protection Act 1998) employees have the right to access their records and the employer is under an obligation to ensure that the data is accurate. Before releasing such data to a third party the employer must seek the permission of the individual concerned.

Storage format of personnel records
In the event that employment contracts/accident record books and other personnel records are needed for the purpose of a legal action, the originals must be made available or the employer must explain what happened to the original documents backed up by what is known as a 'statement of truth'.

Statutory retention periods

Record	Statutory retention period	Statutory authority
accident books, accident records/reports	3 years after the date of the last entry (see below for accidents involving chemicals or asbestos)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended
accounting records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
income tax and NI returns, income tax records and correspondence with the Inland Revenue	not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)
MEDICAL RECORDS	40 years from the date of the last entry	This is all the H&S regulations below
records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677)
records relating to children	until the child reaches the age of 21	Limitation Act 1980
records relating to	6 years from the end of the	The Retirement Benefits Schemes (Information

events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 1995, records concerning decisions to allow retirement due to incapacity, pension accounts and associated documents	scheme year in which the event took place, or the date upon which the accounts/reports were signed/completed.	Powers) Regulations 1995 (SI 1995/3103)
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894) as amended
wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970

Recommended retention periods (ie where no statutory retention periods exist)
Where the recommended retention period given is 6 years, this is based on the 6-year time limit within which legal proceedings must be commenced as laid down under the Limitation Act 1980.

Record	**Recommended retention period**
Pupils' records are live until the day they leave and are kept for 3 years. Paper based records will then go into archive	6 years
Safeguarding children records and those with child protection issues	Kept until the youngest child reaches 21 years. Electronic data will be kept for the same period
Counselling Records are kept in accordance with the client agreement between 1 and 3 years	1 or 3 years according to agreement with the client
actuarial valuation reports	permanently
application forms and interview notes (for unsuccessful candidates)	6 months to a year. (Because of the time limits in the various discrimination Acts, for example the Disability

	Discrimination Act 1995, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months. Successful job applicants documents will be transferred to the personnel file in any event.)
assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	permanently
Inland Revenue approvals	permanently
money purchase details	6 years after transfer or value taken
parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance
pension scheme investment policies	12 years from the ending of any benefit payable under the policy
pensioners' records	12 years after benefit ceases
personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases
redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy
senior executives' records (that is, those on a senior management team or their equivalents)	permanently for historical purposes
time cards	2 years after audit
trade union agreements	10 years after ceasing to be effective
trust deeds and rules	permanently
trustees' minute books	permanently
~~works council minutes~~	~~permanently~~

APPENDIX - 2 CODE OF PRACTICE FOR SHARING PERSONAL INFORMATION

Due to the nature of the work you may be asked at times to share information.

The following notes explain what you need to consider when you are asked to release sensitive/personal information:

1. Set out why you want to share personal information and what benefits you expect to achieve.
2. Provide for a realistic appraisal of the likely effects of the sharing on the people the information is about, and of their likely reaction to it.
3. Give advice on finding alternatives to using personal information, for example using statistical information.
4. Describe the information that you need to share to achieve your objective and the organisations that need to be involved.
5. Outline the relevant legal provisions that require or permit your organisation to share information, or prevent it from doing so.
6. Address any issues that might arise as the result of sharing confidential or sensitive information.
7. Say whether individuals consent for information sharing is needed and if so how to obtain consent and what to do if consent is with held.

Any information sharing must be necessary. Any information shared must be relevant and not excessive. See Appendix 3 – Flowchart of key questions for information sharing.

APPENDIX 3 - FLOWCHART OF KEY QUESTIONS FOR INFORMATION SHARING