Alt Valley
Empowering Communities

GDPR (Data Protection) Policy

Aim

AVCT needs to keep certain information about its employees, learners and other users. It is necessary to process this information so that staff can be recruited and paid, programmes of study organised, statutory obligations to funding bodies and other organisations complied with. To remain within the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The General Data Protection Regulations forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018).

Principles

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability
- These principles should lie at the heart of your approach to processing personal data.

All staff, directors, learners or others who process or use personal information must ensure that they follow these principles. It is intended that this Data Protection Policy will help to ensure this happens.

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies adopted by AVCT at all times. Any failure to follow the policy may therefore result in disciplinary proceedings. Any member of staff or learner who considers that the policy has not been followed in respect of their own personal data should raise the matter initially with their manager/tutor in the first instance.

Notification of Data Held and Processed

All learners, staff and other users are entitled to:

- Know what information is held and processed about them within AVCT and why;
- Know how to gain access to it;
- Know how to keep it up to date;

- Know what is being done within AVCT to comply with the obligations of the Data Protection Act.

Responsibilities of staff

All staff are responsible for:

- Checking that information that they supply to AVCT in connection with their employment is accurate and up to date;
- Informing the Assistant Executive Director of changes to information which they have provided, e.g. change of address;
- Checking the information which will be sent out from time to time, as detailed above; informing the Assistant Executive Director of any errors or changes. AVCT cannot be held responsible for any errors unless notification of those errors has been received.

If and when as part of their responsibilities, staff collect data/information about other people, (e.g.) learners' work, data relating to their ability, references for learners or other staff, or details of personal circumstances, they must comply with the following guidelines.

Data Security

All staff are responsible for ensuring that;

- Any personal data which they hold are kept securely and not taken off site without the permission of the Assistant Executive Director;
- Personal information is not disclosed either orally or in writing, accidental or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter.

Personal information should be:

- Kept in a secure filing cabinet; or
- In a locked drawer; or
- If it is computerised, be password protected; or kept only on a memory stick which is itself kept securely;
- Staff must report immediately, as part of AVCT Whistle Blowing Policy, if they suspect that security of personal data has been compromised.

Parent / Guardian / Carer and Learner Obligations

Parent / Guardian / Carer and Learners must ensure that all personal data provided to AVCT is accurate and up to date. They must ensure that changes of address, etc. are notified to reception/administration as soon as possible.

Rights to Access Information

Staff, learners and other users of AVCT have the right to access any personal data that is being kept about them either on computer or in manual files. Any person who wishes to exercise this right should make a written request to the AVCT Assistant Executive Director or a Director in the first instance. Any other member of staff receiving a request for access to personal data **must** pass on that request to the AVCT's CEO who will ensure that the request is dealt with accordingly.

Where users are not either employees, learners or member of Board of Directors, the request should be in writing and addressed to the CEO; there may well be a charge simply to cover the administration cost of extracting and photocopying the information on each occasion that access is requested. This charge can be waived at the discretion of AVCT's CEO. A secure means of transferring the data relating to a data request will be established. AVCT will inform relevant partners and funders if a data request has been made in line with service level agreements.

AVCT aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 working days, unless there is good reason for delay. In such cases, the delay will be explained to the person making the request.

Publication of AVCT Information

Information that is already in the public domain is exempt. It is policy of AVCT to make the following information available to the public for inspection:

- Names of AVCT Directors
- Names of AVCT's Senior Leadership Team
- AVCT policies

Fair Processing Notice

AVCT has a duty under the Children's Act and other enactments to ensure that staffs are suitable for the job. The AVCT also has a duty of care to all staff and learners and must therefore make sure that, employees and those who use the AVCT facilities do not pose a threat or danger to other users. All staff that are in regular contact with young people or vulnerable adults will undergo a DBS check. The AVCT will also ask for information about particular health needs. The AVCT will only use

the information in the protection of the Health and Safety of the individual, but will need consent to process in the event of a medical emergency, for example.

The Data Controller and Designated Data Controllers
AVCT as a corporate organisation is the data controller under the Regulations, and the Board of Directors is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day-to-day matters. Based on the requirements of delivery contracts AVCT may become the processor.

AVCT's designated data controllers are the Chief Executive and Lead Administrator for personnel data and Centre Manager for learner and curriculum data. In the absence of the Chief Executive, any issues needing urgent attention relating to the provisions of this policy should be raised with the Centre Manager, or other member of the Senior Management Team acting on behalf of the CEO.

Retention of Data
AVCT will keep some forms of information for longer than others. The retention of data is governed in many cases by legislation. For employees this includes information necessary in respect to pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

Conclusion
Compliance with Data Protection 2018 it is the responsibility of all members of AVCT. Any deliberate breach of the data protection policy by AVCT staff may lead to disciplinary action being taken, or access to the AVCT's facilities being withdrawn, or in the most serious cases, a criminal prosecution.

Practicalities

Guidelines for Staff

Data Collection
You must ensure that you only collect data for the purposes for which the AVCT is registered. A data cleanse must take place as directed to ensure that only data legitimately required is held. You should not create any data storage system (e.g. database, spreadsheet, computerised mailing list, or manual filing system) which holds personal data without the knowledge and permission of your line manager. Do not set up, or allow your staff to set up any of the above without the AVCT's Chief Executive in the first instance. You must also notify the Chief Executive of any new systems, or changes to existing systems for the processing of personal data, whether electronic or manual.

AVCT is registered to hold data for the following tasks:

1. Administrative Support – E-mail, security system, office administration
2. Personnel/Employee Administration – Recruitment, payroll, pension, employment related records
3. Purchase/Supplier Administration – Financial details, supplier records, orders, invoices etc.
4. Work Planning and Management – Rotas, project management, vehicle or equipment usage records
5. Public Relations and External Affairs – Promotion of links with external organisations and individuals
6. Marketing and Selling – Advertising, mail shots, promotional campaigns, canvassing
7. Lending and Hire Services – Leasing of materials or equipment, reservation/booking and recall systems
8. Research and Statistical Analysis – Research work, questionnaires, interviews, research analysis
9. Education and training administration – Learner records, examination data, curriculum planning. For example for the purpose of continued learning or to ensure accuracy of information in relation to claims for funding. Learner contact information may be used for research purposes and surveys by funders to ensure consistency of learning and to carry out its functions.
10. Consultancy and Advisory Services – Consultancy, advisory services to employers (This register entry relates particularly but not exclusively to work with employers)
11. Fund-raising – Administration of appeals or other charity fund-raising initiatives. If you are at all unsure as to whether what you want to do is covered, please contact AVCT's Chief Executive.

Responsibility to Data Subjects

You must ensure that when you are asking for information, the supplier of that information knows what it will be used for. For example, if you are collecting data on a form, include a sentence or paragraph which explains the need for the information, and who will have access to it. If you are asking for sensitive data, you must make sure that the subject signs to give 'express consent' for those pieces of data to be collected. If you are unsure about whether the information is sensitive consult the AVCT's Chief Executive.

If you are collecting data by interview, or over the telephone, again ensure that you make clear at the start of the interview that the person that you are talking to understands why you are asking for the information, and what it is to be used for.

Sufficiency

Collect only as much information as is necessary. Be very clear about the intended use of the data, and restrict the data collection to that information which will allow you to carry

out that task. If it is possible to avoid the use of 'personal data', i.e. to work with data from which individuals *could not be identified,* then this should be done. Take every possible step to verify that the information that you are collecting is accurate. Where there are opportunities to check information, e.g. by cross referencing with manual records or by using tolls within your software (spellcheckers, post-code verifiers) then take them. Your data should always be as accurate and up-to-date as possible. Ensure that you have routines to correct any inaccuracies that come to light as soon as they are spotted. It is poor practice to leave data errors uncorrected, and in certain circumstances, can be disastrous, an erroneous digit in a payroll record for example.

Currency

Regularly review the data that you hold, and make sure that information is up-to-date as possible. If your use of the data is ongoing, build in routines which will allow people to update the information that you on them. This can be as straightforward as asking people to notify you of a change of address.

Reports and Analysis

Make sure that any data processing, i.e. production of reports or statistical analysis, is done accurately, and in such a way that will not change or distort your source data. Do not expect untrained staff to carry out complicated statistical tasks, and ensure that **only** those who are entitled to see the information are responsible for working with it.

Retention

The **General Data Protection Regulation** states that personal **data** must be kept "no longer than is necessary for the purposes for which the personal **data** are processed" [Art.5(1)(e)]. Do not hold information for longer that is necessary. The AVCT must be able to justify the storage of any data, at any time. In accordance with statutory regulations, and AVCT policy, archive where necessary, and delete data which is no longer of any use. DO NOT hold on to information just because you feel it 'may come in useful' one day. Seek advice from the Assistant Executive Director as required.

Disclosure

Only pass on information to those who are authorised to see or use it. Ensure that anyone from within the AVCT requesting data has a bona fide need for the information. If you are unsure as to whether you should disclose information internally, consult the Assistant Executive Director for advice. Never give information to an external enquirer without written proof of authorisation. Do not give details over the telephone, and ensure that your staff are aware of this restriction. If you believe that the enquirer has a legitimate right to receive information, and it is not practicable to delay disclosure, in the case of instance, of a police officer investigating an alleged criminal offence, please forward the query to the CEO.

(The only exception to this is in the case of a genuine emergency, in which case the information may be disclosed to the emergency services). Any person, about whom information is within a computerised or manual system in the AVCT, has the right to see whatever information is being held, and to request that it be altered, should they regard it to be inaccurate. The AVCT complies with the Freedom of Information Act; anyone wanting to see their personal information should make a formal request in writing to the CEO in the first instance and via admin@mactac.org.uk. Please refer anyone asking to see his or her data to the CEO.

Security

This is one of the most important aspects of data use, and the one to which all staff should pay close attention. Staff should ensure that where personal information is stored, care is taken wherever possible to restrict access to the data. It should not be possible for people walking in to an office, or walking past a computer screen, to read personal data. Similar care needs to be taken with the location and storage of printouts. Paper based systems containing personal data should be kept in securely. All unwanted data should be shredded and only carried out by staff who understands the importance of security in this context. Computerised systems containing personal data should be fully password protected, the passwords changed regularly, and individuals made aware of the necessity to maintain the secrecy of their personal passwords. Passwords must never be given to learners or unauthorised staff. Users should make sure that unauthorised personnel are not able to read personal data from their computer screens. Users of the network should use only their own login passwords, in order to maintain the security of the network system, and enable an 'audit trail', should the network's security be compromised. Computers that are not in use should be logged out or switched off. Back-ups of data should be regularly carried out, and the back-up media held securely. Unwanted printouts or other files containing personal data should be shredded.

Personal data should be disclosed only to authorised personnel. The long-term storage of AVCT-related personal data off-site is subject to the prior approval of the Assistant Executive Director. Staff working on personal data at home should be aware of the security required for such data, and should ensure that unauthorised access is not given. AVCT software and hardware should not be removed from the premises without prior authorisation. Any perceived breaches of the security of personal data held by the AVCT should be reported immediately to your manager.

Performance Review

Relevant legislation informing the policy

The General Data Protection Regulations 2018
The Data Protection Act 2018

The Freedom of Information Act 2000
The Children's Act 2004

Feedback and further information
AVCT welcomes all constructive feedback on this and any other policy. If you feel that areas of the AVCT's work is not adequately covered by this policy or you need further information/clarification on Data Protection issues please contact
Danielle Forman on 0151 546 5514 or via enquiries@altvalley.co.uk

Appendix 1
Glossary of Terms

The Act – Data Protection 2018

Data - Any information that will be processed or used within or by a computerised or manual system. This can be written, taped, photographic or other information.

Data Subject - The person to whom the data relates.

Data Controller - The person or organisation responsible for ensuring that the requirements of the Data Protection Act are complied with.

Designated Data Controller - Individual appointed by the AVCT to carry out the day-to-day duties of the Data Controller.

Manual System - Any paper filing system or other manual filing system which is readily structured so that information about an individual is readily accessible.

Personal Data - Information about a living person that by itself, or in conjunction with other information which is kept in a manual or computerised system, is sufficient to identify an individual. This information is protected by the Act.

Processing - Accessing, altering, and adding to, changing, disclosing or merging any data will be processing for the purpose of the 2018 Act

Sensitive Data - Information about a person's religion or creed, gender, trade union membership, political beliefs, sexuality, health or criminal record.

Subject Consent - Before processing personal data, the AVCT must have the agreement of the individual to do so. In the case of sensitive data, this must be specific consent, but in other cases, it can be more general.

The Data Protection principles - The underlying principles of the Act that determine what data can be collected, processed and stored. A failure to abide by the principles will be a breach of the 2018 Act.

The Data Protection Commissioner - Person appointed by the government to administer the provisions of the 2018 Act including notification and to provide guidance and assistance to organisations and individuals.

The Data Protection Tribunal - The tribunal established to deal specifically with matters of enforcement under the Data Protection Act.