AVCT Information Management Policy

OVERVIEW

This policy provides an overarching statement of how we will manage the information held in AVCT to ensure security and appropriate usage of data. Information to which this policy refers includes computer data, manual records and CCTV footage. This policy tackles the following key areas:

1. Information Access and Security

2. CCTV Management

3. Records Management

4. Freedom of Information

Guidance has been sought from the Information Commissioner, Liverpool Local Authority and the Records Management Society when compiling this document. This policy will be reviewed every two years. Details of how members of the public can access information can be found within the Publication Policy.

1. INFORMATION ACCESS & SECURITY

Purpose

This policy describes the means by which AVCT aims to preserve confidentiality, integrity and availability of data. It applies to all staff at all levels of the organisation.

Confidentiality: information is accessible only to those authorised to have access.

Integrity: safeguarding the accuracy and completeness of information.

Availability: ensuring that authorised users have access to information when required.

It is acknowledged that the company has legal, statutory and contractual requirements with which it must comply. The organisation complies with the rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection Act.

The senior manager in the organisation allocated overall responsibility for information security is the CEO.
Specialist security advice will be sought where necessary EFSG amongst others will be consulted as a source of such advice, for example for data protection or network security issues.

Organisational Security

Information and asset classification and control
An accurate inventory is maintained of all the assets associated with information systems.
This is the responsibility of the IT Manager.

Personnel security

This is the overall responsibility of the IT Manager in conjunction with the Assistant Executive Director.

Security responsibilities

Security responsibilities are clearly documented and, where appropriate, addressed at the recruitment phase and included in contracts of employment. Personnel screening processes for permanent and temporary staff include appropriate controls (e.g. availability of satisfactory references, confirmation of claimed academic and professional qualifications, independent identity checks). Staff sign a confidentiality or non-disclosure agreement as part of their initial terms and conditions of employment. There is a formal Disciplinary process for employees who violate security policies and procedures and employees are made aware of the action to be taken if they disregard security requirements.

Information security, education and training

Staff receive appropriate training and regular updates in security policies and procedures before access to systems are granted. This includes training in security requirements, controls and legal requirements, as well as in the correct use of information systems (e.g. log-on procedures).

Responding to security incidents and malfunctions

A formal procedure exists for reporting and responding to security incidents, malfunctions and weaknesses. All staff are aware of their responsibilities to note and report such incidents through the proper management channels as quickly as possible. Recovery is carried out only by appropriately trained and experienced staff. Users are made aware that they should not, under any circumstances; attempt to prove a suspected security weakness as this could be interpreted as potential misuse of the system.

Physical and Environmental Security

This is the overall responsibility of the Manager.

Secure areas

Areas in which critical or sensitive information is processed are physically secured to prevent unauthorised access, damage or interference. Control is achieved by conventional security procedures (e.g. doors and windows locked when unattended, external protection for ground floor windows, intruder detection systems). Access to secure areas is controlled and restricted to authorised personnel only.

Equipment security

Equipment is sited or protected to minimise the risk of theft (including security marking), damage (e.g. fire, water, impact), and power failure (e.g. uninterruptible power supply or UPS).

Cabling is protected from interception or damage (e.g. use of conduit, fibre, avoidance of public areas, routed underground, away from communications cables).

Equipment is correctly maintained and serviced by authorised personnel.

Off-site security

Equipment is not taken off-site without authorisation. Where necessary and appropriate, equipment is logged out and backed up by the IT Manager. Equipment and media taken off the premises is not left unattended in public places. Portable computers are carried as hand luggage and disguised where possible when travelling. Home working is subject to suitable controls.

Secure disposal or re-use of equipment

Appropriate arrangements are made for the secure disposal of media containing sensitive information. Confidential paper documents are securely disposed of in line with Records Management guidelines. Storage devices containing sensitive information are destroyed or securely overwritten (rather than using the standard delete function) prior to disposal.

Equipment containing storage media (e.g. hard disks) are checked to ensure that sensitive data and licensed software have been removed or overwritten prior to disposal or re-use.

Clear desk and screen policy

Paper and computer media are stored in suitable locked cabinets where appropriate. Sensitive printed material is cleared from printers immediately and shredded/disposed of.

Business critical information is held in a fire resistant safe or cabinet, PCs and printers are not left logged on when unattended and are protected as appropriate by key locks, passwords or other controls when not in use. Users terminate active sessions and log off when finished. Where appropriate, PCs shut down or time-out after a period of inactivity, with a limited time-out facility afforded by password protected screen savers.

Communications and Operations Management

This is the overall responsibility of the Manager in conjunction with the IT

Manager. Operating procedures are documented and maintained. Changes to systems are controlled with significant changes identified and recorded, following assessment of the potential impact of the change and the change details communicated to the relevant persons. Incident management procedures are in place to ensure a quick, orderly and effective response to security incidents. Protection against malicious software (viruses, etc.)

Software licensing requirements are complied with and the use of unauthorised software is prohibited. Anti-virus detection and repair software is installed and regularly updated.

Electronic mail attachments and downloads and any files of uncertain origin on electronic media or downloaded are checked for malicious software before use. Appropriate business continuity plans for recovery from attack are in place (e.g. data and software back-up and recovery arrangements).

Housekeeping and network management

Back-up copies of essential information and software are taken regularly according to an appropriate schedule. At least two generations of back-up information are retained for important applications and are stored with an appropriate level of physical protection at a sufficient distance to escape a disaster at the main site. Back-up media and restoration processes are regularly checked to ensure that they are effective. Controls are in place to ensure the security of data in networks and the protection of connected services from unauthorised access.

Electronic mail

Guidelines exist on when to use and not to use email. Staff understand the potential difficulties of the difference between electronic and traditional forms of communication (e.g. speed, message structure, degree of informality and vulnerability to unauthorised actions and attack - interception and viruses). Staff understand their responsibility not to use email in such a way as to compromise the good name of the organisation (e.g. defamatory email, harassment, unauthorised purchasing).

Access Control

This is the responsibility of the IT manager.

User registration

Formal procedures are in place to control the allocation of access rights to information systems and services. Users have authorisation from the system owner and the level of access is appropriate for the purpose. User access rights are regularly reviewed; access rights of leavers are removed immediately and redundant user IDs removed. Privileges associated with each system and user are identified, allocated on a need-to-use basis and kept to a minimum.

User password management

Users understand the need to keep passwords confidential and to avoid sharing them, keeping a paper record or recording them in a way that makes them accessible to unauthorised persons. Passwords are changed at regular intervals/30 days or if there is a possibility that security has been compromised, according to a system that ensures use of quality passwords.

Systems development and maintenance

This is the responsibility of the Business Manager in conjunction with the IT Manager.

Security issues are identified and considered at an early stage when procuring or developing new information systems. Input data is validated to ensure that it is correct and appropriate. Outputs and downloaded or uploaded data are checked for validity and integrity.

Business Continuity Management

This is the responsibility of the Manager and IT Manager.

Business continuity management aims to reduce disruption to the running of the organisation that would otherwise be caused by, for example, natural disasters, accidents, equipment failures and deliberate actions. It applies to all business processes, not just those related to information management. Continuity plans, each with an identified owner, are in place within a business continuity planning framework that ensures that all the plans are consistent and a priority order exists.

Compliance

Intellectual Property Rights (IPR)

Appropriate procedures are in place to ensure compliance with legal restrictions in the use of material in respect of which there may be IPR, such as copyright, design rights or trademarks. Software is usually supplied under a licence agreement that limits the number of copies that can be made of the software. Controls are in place including maintaining an appropriate inventory or asset register of software, maintaining proof of licence ownership (e.g. licences, master disks, manuals, etc), controlling the number of users, carrying out checks that only authorised software is in use and applying sanctions against unauthorised copying of software.

Student use of systems

This is the responsibility of the Manager and Lead Verifier. Students sign up to an acceptable use policy.

Sanctions

This is the responsibility of the Senior Management Team in conjunction with the IT Manager. All users – staff, students, other members of the wider community are subject to sanctions if misuse of the systems is encountered.

2. CCTV MANAGEMENT

Purpose & Risk Assessment

The requirement of CCTV has been evaluated and deemed necessary and proportionate in order to support the following objectives:

- to deter and detect unauthorised intruders
- to increase personal safety of students, staff and visitors
- to protect the buildings and assets
- to deter and detect vandalism, damage and disruptive behaviour
- to support the Police in order to deter and detect crime; identify, apprehend and prosecute offenders.

Alternative methods have been considered and other measures are in place as appropriate, including staff supervision of public areas during break times and the requirement to sign in/out. It is acknowledged that CCTV is the only method which can consistently monitor vulnerable areas within the building, acting as a deterrent and assisting with detection when an incident occurs.

Cameras will be placed in locations which are deemed vulnerable to maximise the protection to students, staff, visitors and the Centre. Each location has been assessed and does not pose a threat to personal privacy, avoiding toilets and changing rooms.

Data Protection

The use of CCTV on site has been lodged with the Information Commissioner's Office; this policy has been written with reference to the CCTV Code of Practice. It is fully intended that use of CCTV complies with Data Protection regulations and licensing requirements. The 'Data Controller' is Alt Valley Community Trust.

Staff Access

One monitor will be located within an administration office this will provide the opportunity for cameras to be observed randomly within an area where access is controlled. They are also the nominated individuals who are responsible for downloading recording of incidents should this be deemed necessary.

Signage

Signage will be displayed in key areas to alert all individuals entering the AVCT site that CCTV is in operation.

Data Retention & Recording

Information recorded will be retained digitally for a maximum period of ten days, after which the system will be set to automatically delete the recording without any intervention.

When an incident occurs, one of the staff members listed above must be made aware.

These staff members are nominated to be responsible for intervening and creating a recording of the incident, this will involve downloading the data to a secure area of the network. This data may be shown to the individuals involved, their parents or carers and any other professional agency representatives who are involved in bringing the incident to a satisfactory conclusion.

Where a criminal act occurs a copy of the recording may be provided to the Police. In these circumstances the Police are then deemed to be 'Data Controllers' for their copy of the recording as set out within the Information Commissioner's guidelines.

All information downloaded will be recorded on the electronic CCTV Download Log; this will also show any copies made and the date of deletion, which will be deemed appropriate when the incident has been satisfactorily concluded. Staff members nominated to have access to the system will be responsible for maintaining the log.

Should copies be created E.g. CDs, they will be stored in the safe and shredded when destruction is due.

The board will act as a critical friend to ensure procedures are followed, they will also review this policy and as such will consider whether CCTV usage remains appropriate and continues to support the objectives set out in this policy.

The Centre Manager will be responsible for quarterly checks to ensure the date and time on the CCTV system remain accurate and checking the quality of recording.

Subject Access Requests

Individuals whose images are being recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images.

Individuals wishing to make a Subject Access Request should do so in writing stating the date, time and location of the recording required, giving details by which they can be identified. It should be noted that, in order to comply with data protection, third parties present on the recording may be obscured in the copy provided. AVCT will aim to respond to all such requests within 20 calendar days to comply with statutory guidelines and will charge £10 for providing the data which will be via CD.

Any individual wishing to share feedback or express concerns about the use of CCTV on site should contact one of the staff members nominated within this policy.

This policy is a public document and it is encouraged that anyone enquiring about CCTV usage on site is provided with a copy. The Information Commissioner's Office can be contacted by telephone 08456 306060 or e-mail mail@ico.gsi.gov.uk or on the internet www.ico.gov.uk .

3. RECORDS MANAGEMENT – RETENTION & DESTRUCTION

It is recognised that the efficient management of records is necessary to comply with legal and regulatory obligations in addition to effective running of the Centre This policy applies to all records created, received or maintained by AVCT staff.

Records are defined as all those documents which facilitate the business carried out by AVCT and which are thereafter retained (for a set period) to provide evidence of its transactions and activities. These records may be created, received or maintained electronically or in hard copy. The Centre has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment.

All staff must ensure that records for which they are responsible, or to which they contribute, are accurate and legible and that information is objective and expressed using appropriate language. They should ensure that records are maintained and disposed of in accordance with the records management guidance.

Retention of Records

Under the Freedom of Information Act 2000, AVCT are required to maintain a retention schedule listing each record series which the centre creates in the course of its business.

Destruction of Records

When records have reached the end of their retention period, as set out within the Retention Schedule, they should be disposed of in accordance with confidential disposal guidelines. The schedule refers to shredding of documentation, deletion of electronic data or archiving records for permanent preservation where appropriate.

Shredding means that any hard copy document containing data which identifies an individual should be shredded using a category three cross cut shredder in order to prevent the document being reconstructed.

Deletion means secure disposal – refer to this section within the Information and Access Policy.

AVCT Closure

Should the centre close permanently, records which cannot yet be disposed of should be transferred to the appropriate party i.e. funders, Awarding Organisations for storage and disposal of the remaining records.

4. FREEDOM OF INFORMATION

AVCT has adopted a proactive approach to sharing non-confidential information, access our Publication Policy for details. Any information which is not part of the Publication Policy can be requested under the Freedom of Information Act 2000. This is in accordance with guidance provided by the Information Commissioner and the Local Authority.

To request information, write to the Alt Valley Community Trust Board of Trustees and include the following:

- State that your request is being made under the Freedom of Information Act
- Include your contact name and address
- Give a clear description of what you require

We will aim to supply the information to you within 20 days, unless there is an exemption or a fee to pay.

The AVCT Board will maintain a Disclosure Log to monitor the requests received. This will include the date received, nature of the enquiry and if the response timeframe was met.

It is recommended that guidance about the Freedom of Information Act is accessed prior to making a request, this can be located via: www.ico.gov.uk.