ADULT TRAINING NETWORK

DATA PROTECTION/INFORMATION SECURITY POLICY

(INCORPORATING GDPR)

Details of the ATN Data Protection/Information Systems Security Policy and Procedure

TABLE OF CONTENTS

1. INTRODUCTION

This document presents the many issues that Adult Training Network should consider in establishing effective security policies. This issue is of increasing importance in an environment in which IT systems are interconnected through extended communication networks, as the older physical threats from remote communication, either as the result of deliberate unauthorised access (hacking) or the inadvertent introduction of damaging software (viruses).

Threats to the ATN include:

- natural disasters (e.g. fire and flood) ;
- software errors;
- User errors;
- Hardware failure;
- Unauthorised access by people external to the organisation e.g. hackers);
- Unauthorised use of systems by staff;
- Deliberate damage by staff or outsiders;
- Fraud;
- Tampering;

and can have the following impacts:

- Creating problems in IT systems which prevent the ATN conducting its normal operations properly, for example, the unavailability of critical systems to both staff and students;

- Inefficiency in operations through errors in data;
- Loss of confidence, through publication of information as a result of unauthorised access.

Detailed procedures (Standard Operating Procedures) are also in place and constantly updated to compliment the policies detailed in this document. They address specific security issues and provide detailed procedures to ensure compliance with this security policy.

2. Objective

Adult Training Network acknowledges that information and IT systems are important business assets. To ensure that it remains competitive it must address issues of availability, integrity and confidentiality of information. The objective of this policy is to ensure business continuity and minimize business damage by preventing and controlling the impact of security incidents.

This policy is to ensure that IT systems, including computer systems, network components and electronic data, are adequately protected from a range of threats. This policy covers all aspects of the environment: systems, administration systems, environmental controls, hardware, software, data and networks.

It is the responsibility of the Director to ensure that all staff and students observe this security policy.

3. Physical Security

The physical positioning of IT equipment will be planned with due regard to security considerations. Potential risks from fire, natural disasters and civil unrest need to be assessed and guarded against. The analysis of physical security is not confined only to the accommodation provided for the IT equipment, but also considers potential hazards arising from neighbouring accommodation. The working environment must be maintained in conditions that continue to satisfy standards of physical security and not allow deterioration to occur.

3.1 Electrical Protection

All core components of the IT system must be protected against problems with the power supply via smart Uninterrupted Power Supply units.

3.1 3.2 Fire Protection

IT Services must consider fire as the most prevalent physical security hazard, Fire prevention measures should be applied to the accommodation as a whole.

Limitation of fire hazards will be achieved through the following:

- Automatic fire detection systems;
- Manual fire-fighting equipment;
- Enforcement of safety procedures.

IT Staff must be aware of the fire-fighting equipment, these must be suitable for use with electronic equipment. Where fire-fighting equipment is provided to people in IT areas they should be trained in its location and use, particularly the categories of extinguisher suitable for IT equipment:

- Red - Water - not suitable;
- Black - Carbon Dioxide - suitable;
- Cream - Foam - some may be suitable;
- Blue - Dry chemical powder - this can be used, but leaves a residue which is difficult to remove.

3.1 Natural Disasters

The ATN, via its accommodation strategy, will reduce the threats from natural disasters. There is a range of threats which could lead to equipment damage, with the most likely being:

- Local flooding, including water damage from broken pipes;
- Local landslide or subsidence;
- Exceptional weather conditions.

Obviously, where it is possible to select the site for an IT installation, these hazards should be avoided if possible. In most cases the most likely hazards are those arising from threats within the building, for example, pipe bursts. If possible, IT areas in particular server rooms, should be sited away from such threats or modifications made to the accommodation to reduce the hazards.

4. Physical Access

Locked doors which require special keys or security codes to open will protect sensitive IT areas throughout the ATN. Only authorised personnel will have access to sensitive areas. Procedures are in place to control the access of external personnel (e.g. maintenance engineers, external software installs). Any confidential material (documents, external hard drives, software) are held in secure cabinets, even within IT secure areas, available only to authorised people.

4.1 Security Controls

As far as possible access to all IT equipment areas will be locked preferably by deadlock.

Security controls must be applied to any output device which is routinely used for producing sensitive material; for example, printers which are used to produce confidential reports or computer system logs.

Where printers in ordinary offices or other unsecured accommodation are used to print sensitive information, the equipment is not left unattended while the sensitive information is being produced.

Windows are fitted with metal bars to reduce the risk of a break in.

Motion sensors are installed in all rooms and the premises is protected by an alarm system which is directly linked to a security company and an alarm is raised if security is breached.

4.2 Lockable Cabinets

All media containing sensitive information must be stored in locked cabinets. Access must only be given to authorised personnel and keys are to be kept save and secure.

Media used for data integrity and backup purposes will be stored in secure cabinets or safes that provide protection against fire and other hazards.

4.3 Personnel Access

External personnel that require access to sensitive IT equipment on the premises are to be accompanied by a member of IT Services at all times.

Staff are encouraged to challenge strangers in and around IT areas as they may just as easily be an unauthorised person intending to compromise the security of the IT System.

5 IT Systems Access

The ATN must protect and control access to the IT system by employing a wide range of controls and procedures. These must apply to both staff, students within the ATN who are attempting to access resources they are not entitled to, and to external bodies trying to gain access to our systems.

The ATN must actively promote the fact that it is a criminal offence for an unauthorised person to attempt to access a system or information within the system or to attempt to exceed the level of access or privileges granted to them. Action taken in light of the above would be carried out as documented within the ***Computer Misuse Act 1990.***

The purpose of secure system access is to ensure that only authorised personnel gain access to the ATN's computer systems with defined user identification and password schemes.

5.1 Outline of procedures

Detailed in this policy is an overview the main procedures that are in place to ensure that the system can identify each user, control their access through the use of passwording and determine which areas of the system they are entitled to use.

5.1.1 Identification

The use of a unique identifier (user identity) must apply to all users of the system. Generic usernames will be set up for students. A user will only be issued with a user identity if authorisation process has been followed.

All staff users of the network must be authorised via the Manager.

All staff users of the network that require access to the ATN's sensitive data must be authorised via the Manager and then by the Director.

User identities for staff on temporary contracts must contain a cut-off/expiry date for the user identity; this must be supplied prior to the user identity being created.

User identities for both staff and students are removed/disabled promptly when they leave the ATN, are no longer required or there is reason to suspect misuse/abuse.

5.1.2 Passwords

To enhance password security, users must follow good security practices in the selection and use of passwords.

Default Password
Staff users who are given a default random password when the account is created will be required to change it at first login.

5.1.3 Password Requirements

- Minimum digits: the password must contain at least 6-8 characters.
- Minimum alphabetics: the password must contain at least 4 alphabetic characters (a-z, A-Z)
- Passwords must be changed after 30 days (Staff Only).
- Passwords can not be one of the previous eight used.
- An account will be locked out after three bad attempts.

Intruder Detection
Users will be locked out indefinitely after three bad login attempts. A member of the IT Services team should carry out the unlocking of the user account.

Password Uniqueness
Staff Users should not be able to use the eight previously used passwords.

Password Ageing
It is important that passwords are changed regularly. The maximum password age should be set to at most 60 days. Users should be forced to change their passwords every 60 days. Users should be given warnings before the change is required.

Administrator Password
The Administrator password must be changed more frequently than normal users, the administrator has access to restricted areas on all servers. The password is changed on the last Friday of each month and is only given to members of the IT team who require access to make changes.

Summary of Password Policy
Passwords should contain characters from at least three of the following four classes:

English Upper Case Letters A, B, C, ... Z
English Lower Case Letters a, b, c, ... z

Westernized Arabic Numerals 0, 1, 2, ... 9
Non-alphanumeric ("special characters") For example, punctuation, symbols. ({}[],.<>;:'"?/|\`~!@#$%^&*()_-+=)

- Passwords may not contain e-mail names or any part of user's full names.
- Passwords should be changed every 60 days.
- Passwords should never be the same as any of your last eight passwords.
- Password should not be a "common" word (for example, it should not be a word in the dictionary or slang in common use).

A complex password that cannot be broken is useless if you cannot remember it. For security to function, you must choose a password you can remember and yet is complex. For example, Msi10!YOld (My Son is 10 years old).

Password Protected Screen Savers
Password protected screen savers are implemented on all staff computers to reduce the risk of unauthorised access to an unattended computer. The time period to activation is 10 minutes.

MIS Passwords
Sensitive information is further protected by a secondary username and password. Staff users are required to have this additional password to log onto the ATN system. Passwords must be changed after 99 successful logins. Account lockout must occur after 3 unsuccessful login attempts.

Procedures are in place to ensure that only authorised personnel are issued with this secondary password to access sensitive data.

User identities and passwords are removed/disabled promptly when a member of staff leaves the ATN and, no longer requires access or there is reason to suspect misuse/abuse.

5.1.4 User Privileges & Access Rights

The user identifier should be used to determine the particular rights the user has in using the computer system. There will be resources to which only certain users can gain access. User privileges control whether a user has:

- Visibility of the directory entry for a particular file;
- Read access to a file;
- Write access to a file;
- Power to create or delete a directory;
- Power to delete a file.

The access to particular files is controlled in terms of the operations which a particular user may be allowed to perform. The default for all files is that only the owner (Administrator) has access to the information, but that they can assign those rights to others.

5.1.5 Use of User Groups and Organizational Units

The use of groups must be extensively used throughout ATN's IT system in order to simplify the assignment and withdrawal of privileges for a user or group of users.

User privileges are assigned against the group and inherited by the group members. This facility is also useful for system areas where a group of people will need to share access to particular files. Using groups to define access privileges is recommended in favour of simply letting all the users work under the same user identifier. The latter undermines user accountability and must be discouraged.

Administrative Groups

Users placed into administrative groups must be strictly controlled. Only users that specifically require higher level access should be made a member of any administrative group, this would usually be limited to members/managers of the IT Team. Administrative tasks should be segregated according to the task and role it is to administer. Users should be made members as when they are required to carry out such roles.

Administrative group membership should be revoked immediately the user no longer requires or is responsible for the task designated to a particular group.

Users with non-standard access

All users should have their accounts made non-functional when they cease employment with ATN for whatever reason. This must happen immediately notification is given from the Human Resources department.

Standard operating procedures should also be in place for the immediate disablement or removal of any accounts that have any access to network resources above those of a 'standard user'. In particular any users that have administrative access or have access to password information or data that is deemed to be 'sensitive' should be dealt with immediately. Passwords must be changed immediately for any account that the user had access to and password documents updated at this time.

The IT department should document all users that fall into this category and pass this information to the Human Resources. Human Resources should inform the IT engineer when a resignation is received or disciplinary action that could result in suspension or termination of employment from the ATN of any user on this list.

5.1.6 Restrictions on System utilities

Certain system utilities can allow an experienced computer user access to information which may not normally be available. Examples include:

- File Analysis Programs;
- Database Administration Tools;
- Debugging Tools;
- Program Development Environments.

Where possible system policies are imposed on users of the system to limit the use of such utilities unless specifically required for work that needs to be carried out or for teaching purposes.

5.1.7 Restricting database access

Database management systems provide major functionality for the storage of information and their use is common throughout the ATN. These systems support a range of security mechanisms, ranging from password protection for initial access to restrictions on particular data items. Where sensitive information is held, it is recommended that protection be applied to each database entity. Each user can be given privileges which reflect the nature of the access to which they are entitled. This would include:

- Whether a particular user can view certain data;
- Whether a particular user can modify certain data;
- Whether a particular user can create new records within the database;
- Restrictions on particular database operations.

These controls should ensure that only authorised personnel can gain access to sensitive information. These controls can also be used to ensure that system efficiency is maintained, by preventing inexperienced users from accidentally issuing queries which appropriate significant resources.

5.1.8 System log-on procedures

Access should be restricted to all computers within ATN, through password protection. Users enter a security dialogue and are asked for their user identifier followed by the password. These are checked against a list of user identifiers to ensure a legitimate entry has been provided. Even where a legitimate identifier is offered, there may be limitations upon access.

Until the log on sequence has been completed, the user will have no access to any of the computer facilities, as any response may be of benefit to the unauthorised user. If the user fails to provide the correct information they are allowed 5 attempts, after which time no further attempts are accepted until there has been intervention from system administration. All attempts to log in are logged and where there have been unsuccessful attempts.

In some situations, IT systems within ATN offer 'guest' log in facilities in which no password is required or a published password is accepted. These are used to provide information services, for example through Internet sites. Given the

potential damage that an unauthorised user could do if the guest access gave them a channel to protected areas, such facilities are tightly controlled.

5.1.9 Logging Off

Users must be encouraged to log out when a machine is not in use, as a live terminal which has been left unattended is a significant opportunity for unauthorised access. The computer system should have facilities to force a log off if a particular terminal has been inactive for a long period of time, this is of particular importance on all computers that are used by members of staff.

5.1.10 Audit Trails & System Logs

Maintaining security is supported through the use of system audit trails and logs. The usage of systems must be routinely logged so that all unauthorised use can be identified. Items to be recorded include:

- Major system activities (e.g. system crashes);
- User log in attempts;
- Log offs;
- Users attempting to access facilities outside their privileges;
- Users attempting to access information belonging to others;
- Password changes.

The logs will be examined on a regular basis, viewing a sample manually and using a file analysis program to search for significant events. The logs are retained for a period of time.

Where possible analysis of the logs will happen in real time and notify IT Services of specific events that may represent a security risk.

5.1.11 Computer misuse awareness

The Computer Misuse Act 1990 makes it a criminal offence for an unauthorised person to access or misuse a computer and all the ATN staff need to be aware of this. Obviously, this will not prevent unauthorised use, but it does provide a psychological hurdle for those considering misuse of the IT system and provides grounds for pursuing criminal action should the need arise.

*See computer use policy.

6 Unauthorised Software

The ATN is committed to the use of authorised software only within its computer systems. It is expressly forbidden for people to load or operate software gained from the Internet, magazine gifts or other sources. The organisation is also committed to using software for which it has current licenses only and will not accept the use of more copies of a particular piece of software than it has licences.

PC users are made aware that only software authorised by the ATN can be used. This is backed up by regular software audits to check that unauthorised software is not being used.

It is the personal responsibility of all users to ensure that they do not introduce viruses into computer systems. They should take care when receiving electronic information from an unknown source, including attachments within e-mail. Where there are reasons to bring information from a questionable source and active virus checking should be performed.

6.1 Unlicensed software

The ATN can only protect itself against users making extra copies of licensed software or obtaining copies from external sources through the application of control procedures. The ATN will audit each user's PC and establish exactly which programs they have available to them.

The overall number of copies of a particular item identified by the audit should be reviewed against the number of licences the ATN should have available to it. If infringements are found, the users should be notified and the offending items removed. This will be legitimising the use through the purchase of further licences or the removal of the offending software.

The ATN informs users that copies of software or the introduction of software packages from sources outside the organisation is expressly prohibited.

Where possible site licenses are used for software that may be difficult to quantify, this is an effective way of reducing or eliminating the risk of inadvertently breaking a license agreement.

6.2 Virus protection

The ATN uses Anti-Virus software to safeguard its systems from malicious code. All discs, cd-roms or other transportable media must be virus checked prior to use on ATN equipment. No material downloaded from the Internet or received as an email attachment may be used on ATN systems, before being scanned for viruses.

Anti-virus software runs permanently on all servers and computers it is updated with the latest virus information on a weekly basis. Any user who wishes to load any file from any transportable media or external source, must virus check the file before loading. If you require assistance contact the IT engineer

If a virus has been detected within one computer, cleansing, deletion and notification to member of IT Services automatically takes place. All servers have up-to-date anti virus software installed and correctly configured.

7 Personal Computer Security

It is the responsibility of each PC user to take all reasonable precautions to safeguard the security of the computer and the information contained upon it. This includes protecting it from physical hazards, including spilling liquids; not allowing unauthorised users access to the machine and only using approved software.

Special consideration is given to the protection of portable computers, as these are more open to theft and physical damage (e.g. being dropped). Sensitive information must not be stored on the hard disk of a portable computer under any circumstances.

The user of a ATN PC has a level of control over the machine appropriate to their position and needs. They are generally not able to introduce data and software into the PC, tailor the working environment or change the hardware configuration.

7.1 Personal Computers

Computers throughout the ATN are, typically, kept in open offices, classrooms, learning centres or are carried by the individual, and open to a number of threats:

- Theft of the computer or its peripherals;
- Theft or damage to information stored on the computer;
- Accidental or malicious damage;
- The possibility of display screens being overlooked.

The risks will be reduced through the adoption of secure practices:
Keys - classrooms and offices must be locked when not in use. Students must never be left unattended in computer rooms.

Password protection - is available for all PCs. All the ATN's PCs are configured to prevent booting from floppy disk.

Screen locks - are in place on all PCs.

Disc restrictions - users are made aware that their hard disks do not provide a secure storage medium, particularly where portable computers are concerned. The ATN requires all PC users follow procedures which protect any sensitive information they may hold. Measures include:

- Using encryption for any sensitive information held on hard disk;
- Using password protection on any files which hold confidential information;
- Storing information on a networked file server.

7.2 Portable computers

The increasing use of portable computers has generated extra security risks.

7.2.1 Guidelines for the security of portable computers

Users of portable computers within the ATN should follow the guidelines below:

- Do not leave portable computers unattended.
- Store portables in secure cabinets when not in use.
- The users of portables should be vigilant in public places, as theft is common.
- No sensitive information should be held on the hard disk.
- Any floppies containing sensitive information should not be held with the computer.
- Use a carrying case to reduce the risk of accidental damage.
- Ensure that backups are taken.
- Use only legitimate software.

8 Network Security

The ATN recognises the additional security hazards posed by networked systems and wishes to reduce these threats wherever possible. There are sufficient safeguards implemented to prevent unauthorised persons from accessing our IT systems and where there is a need to interwork with the public network there are 'firewalls' installed.

ATN campuses are interconnected via communication networks. This both increases the complexity of the IT environment and creates new forms of security threats. As always, the weakest link in the chain determines the overall security level of the system.

9 Internet Security

While the ATN is committed to use of the Internet for business purposes and student research, it must ensure that suitable controls are in place to prevent security breaches or other negative consequences. The networks used for the Internet are not secure and any communications sent by this means could be accessed or modified by unauthorised individuals.

There are also threats from obtaining information from the Internet, with virus attachments being the most common. Consequently, ATN has adopted procedures, which minimise the risk of using the Internet and follow good practice in the way individuals behave and the Internet sites that they visit.

Where material is obtained from the Internet, users must ensure that any copyright restrictions are obeyed and that virus protection procedures are followed.

It is recognised that the Internet is an area that is undergoing significant technological change and the policy will be reviewed periodically to ensure that it continues to satisfy our needs.

9.1 Internet Security

The Internet is only accessed via proxy/firewall server.

9.2 Firewalls

The ATN by its very nature (Internet and multiple site connections) needs to have connection between an internal network and external communications, a measure of protection can be gained through the use of firewall:

- **Zone Alarm Pro**

The ATN's Firewalls monitor and restrict the communication traffic and tests whether it is being conducted for a legitimate purpose.

10 Backup and Recovery Procedures

The ATN strategy will be to perform weekly full backups. Data is backed up onto an external hard drive and placed in the fireproof safe.

10.1 Systems Testing

The ATN shall be entitled to a number of Systems Testing periods in any Year. We have a separate testing environment and all changes are tested in the test environment before being introduced to the live environment.

11 Individual Responsibilities

Everyone granted access to ATN's computer information systems is responsible for protecting its information assets, systems and infrastructure. Users will protect likewise the information assets of third parties whether such protection is required contractually, legally, ethically or out of respect for other individuals or organisations. They will at all times act in a responsible, professional and security-aware way, maintaining an awareness of and conformance with this Policy.

All members of staff within ATN are responsible for reporting problems and concerns in existing security practices and/or improvements that could be made to the Director.

All members of the ATN who have supervisory responsibility are required to promote security awareness amongst their supervised staff or students.

The Director is responsible for the implementation of the policy and is authorised to pursue appropriate programmes, activities and actions consistent with this security policy that contribute to achieving ATN's security objectives.

Actual or suspected security incidents will be reported promptly to the Director of ATN, who will manage the incident to closure, and analyse it for lessons to be learnt.

The Network Engineer will carry out risk analysis techniques to identify security risks and their relative priorities. Identified risks will be responded to promptly, implementing safeguards that are appropriate, effective, culturally acceptable and practical.

12 Discipline

Breach of the restrictions detailed in this policy may result in the application of the ATN's Disciplinary Procedures and could give rise to criminal and/or civil liability.

This Policy and compliance with it applies to all members of Adult Training Network and those who use its computer and information systems.

13. Additional policy issues

- ATN observes fully the conditions regarding the fair collection and use of personal data
- ATN meets its obligations to specify the purposes for which personal data is used
- ATN collects and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- Ensure the quality of personal data used
- Apply strict checks to determine the length of time personal data is held
- Ensure that the rights of individuals about whom the personal data is held, can be fully exercised under the Freedom of Information Act
- All USB's are encrypted and CD's are password protected which hold clients personal data. ATN is currently using TruCrypt for encryption of sensitive data.
- Take the appropriate technical and organisational security measures to safeguard personal data.
- Lockable filing cabinets are used to store client files. Only authorised personnel are allowed access to personal information of clients and filing cabinets. Further, there are named keyholders for accessing client files.
- No more than 100 pieces of customer data on any spreadsheet is permitted.
- No emailing of NI numbers and group customer data in any correspondence is permitted.
- A unique identifier number to refer to the customer has been implemented over several years.

- Destroying data and hardware which is not in use.

- Time outs are implemented when computers are inactive (5 mins of inactivity) and screen savers are a sign of timeout being activated.

- A clear desk policy is in place. No personal data is permitted on desks when not in immediate use.

- Anti virus and anti spyware ESET Nod 32 Business Edition (Version 4) is currently in use on all computers

- ATN uses Smoothwall (Firewall) corporate edition which protects the internal network. It also incorporates Vipra software which scans files while downloading to prevent malware from infiltrating the system.

- Fax usage is restricted and staff are required to communicate with the recipient before sending faxes to ensure that the appropriate individual receives the information.

- ATN ensures that personal data is not transferred outside the organisation without safeguards. Currently the policy is not to transfer the data off site.

14. GDPR

The General Data Protection Regulation, which came into effect on 25th May 2018, has changed the way we deal with data as it has replaced the former Data Protection Act. Because of this, there are new regulations on how we use and process personal data. ATN is responsible to ensure that the personal data collected is processed fairly and done so in accordance to the law.

We will process data in line with our privacy notice in regards to job applicants, employees and those who access the services provided by ATN.

For more information about ATN's GDPR action plan and how ATN retains data, please visit the ATN website which can be accessed on: http://www.adult-training.org.uk/policies.html

Reviewed by S Singh Gill
Managing Director
Reviewed on 1st April 2019
Date of next review April 2020