Academy Technical Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The academy will be responsible for ensuring that the academy infrastructure and network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the academies policies)
- access to personal data is securely controlled in line with the academies personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of academy computer systems
- there is oversight from senior leaders and these have impact on policy and practice

If the academy has a managed ICT service provided by an outside contractor, it is the responsibility of the academy to ensure that the managed service provider carries out all the e-safety measures that might otherwise be carried out by the academy itself (as suggested below). It is also important that the managed service provider is fully aware of the academy E-Safety Policy and Acceptable Use Agreements). The academy should also check The Education Fellowship's guidance on these technical issues.

Responsibilities

The management of technical security will be the responsibility of the network manager, systems manager or most senior technician or in the case of a managed service, the contractor for those services.

Technical Security

Policy statements

The academy will be responsible for ensuring that the academy infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities. Academies will have very different technical infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational and administrative staff before these statements are agreed and added to the policy:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the academy systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to academy technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager/Technical Staff and will be reviewed, at least annually, by the E-Safety Committee (or other group)
- Users will be made responsible for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The Network Manager (or contractor) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. Inadequate licencing could cause the academy to breach the Copyright Act which could result in fines or unexpected licensing costs

- Mobile device security and management procedures are in place where mobile devices are allowed access to academy systems
- Academy technical staff regularly monitors and record the activity of users on the academy technical systems and users are made aware of this in the Acceptable Use Agreement
- Remote management tools may be used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual/potential technical incident to the E-Safety Coordinator/Network Manager / Technician (or other relevant person, as agreed)
- Where applicable, an agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the academy system
- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on academy devices by users
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on academy devices that may be used out of academy
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on academy devices
- The academy infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, Trojans etc
- Personal data cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all academy technical systems, including networks, devices, email and Virtual Learning Environment (VLE). Where sensitive data is in use – particularly when accessed on laptops – academies may wish to use more secure forms of authentication e.g. two factor authentication such as the use of hardware tokens and if so should add a relevant section in the policy. Where this is adopted, the policy should state clearly that such items as hardware tokens must be stored separately from the laptop when in transit – to avoid both being lost / stolen together.

Policy Statements

All users will have clearly defined access rights to academy technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).

All academy networks and systems will be protected by secure passwords that are regularly changed. The "master/administrator" passwords for the academy systems, used by the technical staff must also be available to the Headteacher/Principal or other nominated senior leader and kept in a secure place e.g. academy safe.

Consideration should also be given to using two factor authentication for such accounts.

Academies should never allow one user to have sole administrator access.

Passwords for new users and replacement passwords for existing users will be allocated by the network manager. Academies may wish to have someone other than the academies technical staff carrying out this role e.g. an administrator who is easily accessible to users. Any changes carried out must be notified to the manager of the password security policy (above).

All users (adults and young people) will have responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Users will change their passwords at regular intervals – as described in the staff and student/pupil sections below.

The level of security required may vary for staff and student/pupil accounts and the sensitive nature of any data accessed through that account.

Requests for password changes should be authenticated by the responsible person to ensure that the new password can only be passed to the genuine user (the academy will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil/student).

Staff passwords

All staff users will be provided with a username and password by the network manager or other designated person who will keep an up to date record of users and their usernames.

The password should be a minimum of 8 characters long and must include three of the following: an uppercase character, a lowercase character, a number, a special character. They must not include proper names or any other personal information about the user that might be known by others.

- The account should be "locked out" following six successive incorrect log-on attempts
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of academy
- Should be changed at least annually. Some academies may enforce required changes more frequently. The frequency should depend on the nature of the account and how sensitive/damaging loss of data would be. It would be reasonable to require staff password changes more frequently that student/pupil password changes
- Should not re-used for 6 months and be significantly different from previous passwords. The last four passwords cannot be re-used
- Should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- Should be different for systems used inside and outside of academy

Student/pupil passwords

Primary academies will need to decide at which point they will allocate individual usernames and passwords to pupils. They may choose to use class logons for KS1 (though increasingly children are using their own passwords to access programmes). Academies need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network/internet access. Academies should also consider the implications of using whole class logons when providing access to learning environments and applications, which may be used outside academy.

All users (at KS2 and above) will be provided with a username and password by the network manager or designated person who will keep an up to date record of users and their usernames. Users will be required to change their password regularly.

Students/pupils will be taught the importance of password security. The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Academies may wish to add to this list for all or some students/pupils any of the relevant policy statements from the staff section above.

Training/Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the academies password policy

- at induction
- through the academies e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the academies password policy:

- in lessons
- through the Acceptable Use Agreement

Audit/Monitoring/Reporting/Review

The responsible person will ensure that full records are kept of:

- User IDs
- User logons
- Security incidents related to this policies
- Joiners/Leavers

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use.

It is important that the academy has an up to date filtering policy which manages risks and provides where possible preventative measures to safe guard the academy, staff and students.

Many users are not aware of the flexibility provided by many filtering services at a local level for academies. Where available, academies should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

Academies to consider carefully the issues raised and decide:

- Whether they will use the provided filtering service without change or to allow flexibility for sites to be added or removed from the filtering list for their organisation.
- Whether to introduce differentiated filtering for different groups/ages of users
- Whether to remove filtering controls for some internet use (e.g. social networking sites) at certain times of the day or for certain users.
- Who has responsibility for such decisions and the checks and balances put in place
- What other system and user monitoring systems will be used to supplement the filtering system and how these will be used

Responsibilities

The responsibility for the management of the academies filtering policy will be held by the network manager or other designated person. They will manage the academy filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the academy filtering service must:

- be logged in change control logs
- be reported to a designated member of the Senior Leadership Team

All users have a responsibility to report immediately to the designated person any infringements of the academies filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the academy. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the academy to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the academy network, filtering will be applied that is consistent with academy practice.
The academy maintains and supports the managed filtering service provided by the Internet Service Provider (or other filtering service provider)

- The academy has provided enhanced/differentiated user-level filtering through the use of the filtering programme allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher/Principal (or other nominated senior leader).
- Mobile devices that access the academy internet connection (whether academy or personal devices) will be subject to the same filtering standards as other devices on the academy systems

- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group

Education/Training/Awareness

Pupils/students will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset

Parents will be informed of the academies filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions/newsletter etc.

Security Requirements for Academy Networks

The following protocols must be enforced by each secondary academy:

- All executable and batch files must be blocked
- Access to the Windows Control Panel must be blocked
- C:\ drive or other drives that are not authorised for users' use must not be visible or accessible
- Computers must have a network connection in order to be logged in
- Unplugged cables must lock workstations
- Students may only login to one machine at a time
- No saving on the desktop must be allowed
- Mandatory profiles must be enforced
- No roaming profiles must be allowed
- Data may only be saved onto the network
- Drives should be mapped though group policy where possible
- The minimum operating system for internet accessible workstations is Windows 7