**St Marys C of E School**

**School Technical Security Policy**



**Date reviewed: July 2015**

**Signed: Headteacher:**

**Signed Chair of governors:**

**Date for next review:**

**Rationale**

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / 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 school’s policies).

• access to personal data is securely controlled in line with the school’s 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 school computer systems.

• there is oversight from senior leaders and these have impact on policy and practice..

If the schoolhas a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that might otherwise be carried out by the *school* itself (as suggested below). It is also important that the managed service provider is fully aware of the *school* Online safety Policy / Acceptable Use Agreements). The *school* should also check their Local Authority guidance on these technical issues.

* St Marys C of E Primary School has a managed ICT service provided by ICT 4, Redruth. An ICT 4 technician is part of the e-safety committee and has regular updates about school policy involving ICT and E-safety.

**Responsibilities**

The management of technical security will be the responsibility of Mr D King (Computing Coodinator), the Headteacher Mrs H Tyreman and a ICT4 technician.

Technical Security

The school will be responsible for ensuring that the school infrastructure / 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:

**• School technical systems will be managed in ways that ensure that the school meets recommended technical requirements** (these may be outlined in Local Authority / other relevant body technical / online safety policy and guidance)

• **There will be regular reviews and audits of the safety and security of school academy technical systems**

**• Servers, wireless systems and cabling must be securely located and physical access restricted**

**• Appropriate security measures are in place** (schools may wish to provide more detail) **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 school systems and data.**

**• Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff** (schools may wish to provide more detail).

**• All users will have clearly defined access rights to school / academy technical systems.** *Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually, by the Online safety Committee (or other group).*

*•* Users will be made responsible for the security of their username and password, 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. *(See Password security policy).*

*•* Mr D King and ICT 4 are 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.

*•* Mobile device security and management procedures are in place. (See A.U.Ps for adults and children, and the Guidance to accompany the A.U.Ps with the sanction policy attached).

• School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

• Remote management tools are used by staff to control workstations and view users activity

• An appropriate system is in place (through email or the use of Whisper on the school website) for users to report any actual / potential technical incident to the Online safety Coordinator / Network Manager / Technician (or other relevant person, as agreed).

• An agreed policy is in place (Guest logons can be provided after A.U.Ps have been signed, but guest cannot access restricted or confidential files or folders) for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school system.

*• An agreed policy is in place* (All staff and children must consult the ICT Coordinator before installing any files) *regarding the downloading of executable files and the installation of programmes on school devices by users*

*• An agreed policy is in place* (see Adult A.U.Ps and Accompaning guidance documents) *regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.*

*• An agreed policy is in place* (see E-safety Policy and A.U.Ps plus guidance document) *regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.* (see School Personal Data Policy for further detail.

*• The school 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 school site unless safely encrypted or otherwise secured.* (see School Personal Data Policy)

Further Guidance

35

Schools / academies may wish to seek further guidance. The following is recommended:

NEN Technical guidance: <http://www.nen.gov.uk/advice/266/nen-guidance-notes.html>

.