Appendix2:
School 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 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 is oversight from senior leaders and these have impact on policy and practice.

Technical Security

Policy statements

- As a Bolton school, our school subscribes to Bolton Schools ICT (Bolton SICT) Broadband services; internet access is via the local authority maintained Wide Area Network.
- There is a central internet filtering system for all schools.
- This is an industry standard solution, Sophos Universal Threat Management, the product incorporates the IWF standards.
- This is configured as per DFE guidelines, see following technical blog post:
- https://technical.bolton365.net/internet-filtering/
- The system can also be deployed at school level if required, but the standard configuration has distinct filtering levels for staff and pupils.
- Filtering change requests are online and are only accepted from authorised users. Any changes are security checked before implementation.
- The system provides Bolton SICT with full monitoring and reporting, these reports are available to schools when requested.

Bolton SICT Broadband service also includes:

- ✓ Email content filtering
- ✓ Email anti-spam
- ✓ Secure email facilities
- ✓ Full anti-virus
- ✓ Encrypted document exchange
- ✓ 2 factor remote access
- ✓ Industry standard firewalls to protect both WAN and school LANs

- Bolton SICT staff that maintain these systems are all minimum Microsoft qualified and have many years industry experience.
- Pupils from Year 2 onwards use individual logins to allow monitoring of computer usage.

- From EYFS, for network, Purple Mash and blog logon, pupils use a password.
- Further information about the technical security of services can be requested by emailing: contact@sict.bolton.gov.uk
- For devices, such as iPads, that do not do not use network logins, BSICT are currently looking at ways of user authentication to provide monitoring.