THE WHITE HORSE FEDERATION

IT Technical Security

Key Document details:			
Author:	Mark Weller	**Approver:**	CEO
Owner:	Mark Weller	**Version No.:**	2.0
Date:	10/11/2017	**Next review:**	Annual
Ratified:	10/11/2017		

Technical Security

The WHFIT Support Team, school staff and departmental managers 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.

- School/Academy technical systems will be managed in ways that minimise risk. The Head of ICT & Communications will be responsible for ensure procedures are in place that technical staff adhere to.
- There will be regular reviews and audits of the safety and security of school technical systems. These will be carried out by the WHFIT Support Team aided by ICT staff members within the school. Any findings will be presented to SMT/ SLT with appropriate recommendations.
- 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 school 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 school / academy technical systems.
- The WHFIT Support Team 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.
- An appropriate Mobile Device Management (MDM) system will be used for mobile device security and management.
- School / academy 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 for users to report any actual / potential technical incident to the online safety co-ordinator / WHFIT Support Team / online safety lead
- An agreed local school policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans, etc.

The following policy / procedure will be followed for the provision of temporary access to the schools network or Internet connection.

School/ Establishment:

<enter details here>