Wootton-by-Woodstock

ODST
Oxford Diocesan
Schools Trust

Wootton-by-Woodstock CE Primary School

Policy Agreed: Jan 2019
Person Responsible: Jo Palmer
To be reviewed: Jan 2022

Policy for ICT Security 2019

INTRODUCTION

Effective technical security depends not only on technical measures but also on appropriate procedures and on good user education and training. The headteacher and the local governing body are responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only have access to 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 this policy
- There is effective guidance and training for users
- There are regular reviews of the safety and security of school computer systems
- There is oversight from the headteacher, governors and the computing coordinator and these have impact on policy and practice.

RESPONSIBILITIES

The school has a managed ICT service provided by an outside contractor which carries out all the online safety measures on our behalf. The service provider is fully aware of the school e-safety Policy and Acceptable Use Agreements.

The management of technical security in Wootton-by-Woodstock School is the responsibility of the headteacher.

ICT SECURITY

Wootton-by-Woodstock Primary School is responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved by the local governing body are implemented. We also ensure that the relevant people receive guidance and training and are effective in carrying out their responsibilities.

TECHNICAL SECURITY CHECKLIST

Checklist	In Place	Partially	Not in Place
School technical systems are managed in ways that ensure that the school meets recommended technical requirements as outlined in the e-safety policy.			
There are regular reviews and audits of the safety and security of school technical systems			
Servers, wireless systems and cabling are securely located and physical access restricted.			

Checklist	In Place	Partially	Not in Place
Appropriate security measures are in place to protect the 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 technical systems. Details of the access rights available to groups of users are recorded by the Network Manager / Technical Staff (or other person) and are reviewed, at least annually, by the local governing body (LGB).			
Users are taught about and made responsible for the security of their username and password and do allow other users to access the systems using their log on details. They know what to do if there has been a breach of security.			
A named member of staff is responsible for ensuring that software licence logs are accurate and up to date.			
Mobile device security and management procedures are in place for school provided devices and / or where mobile devices are allowed access to school systems.			
School leaders/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.			
An appropriate system is in place for users to report any technical incident to the Network Manager / IT Leader.			
An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school system.			
An agreed policy is in place regarding installation of programmes on school devices by users			
An agreed policy is in place (iPad and laptop agreements for staff) regarding the type of use on school devices that may be used out of school.			
An agreed statement is in place (in the ICT Security Policy) regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices			
The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc			

Checklist	In Place	Partially	Not in Place
Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured			

PASSWORD SECURITY

A safe and secure username and password system is in place. Where sensitive data is in use, the programs we use requires more secure forms of identification.

Pupils have individual usernames for the system.

PASSWORD SECURITY CHECKLIST

Checklist	In Place	Partially	Not in Place
All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users are recorded by the school business manager and are reviewed, at least annually, by the LGB.			
All school networks and systems are protected by secure passwords that are regularly changed			
The "master / administrator" passwords for the school systems, used by the technical staff is available to the Headteacher or other nominated senior leader and kept in a secure place e.g. school safe.			
All users (adults and where issued, pupils) have responsibility for the security of their username and password know they 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.			
Passwords for new users, and replacement passwords for existing users are allocated by a named member of staff (MW)			
Staff Passwords			
All staff users are provided with a username and password by a named member of staff who will keep an up to date record of users and their usernames.			
Staff passwords are changed regularly			
Pupil Passwords (where issued)			
All users (at KS2 and above) are provided with a username and password by a named member of staff who will keep an up to date record of users and their usernames			
Users are required to change their password every academic year.			
Students / pupils are taught the importance of password security			

Users are made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This applies to even the youngest of users, even if class log-ins are being used.

Members of staff are made aware of ICT security:

- At induction
- Through the school's e-safety policy and this policy
- Through the Acceptable Use Agreements.

Pupils are made aware of the school's password policy

- In lessons
- Through the Acceptable Use Agreement.

FILTERING

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or inappropriate in an educational context. Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the filtering provider by actively employing the illegal content lists. Filter content lists are regularly updated, and internet use is logged in planning and children's use monitored. The monitoring process can alert the school to breaches of the filtering policy, which are then acted upon. Changes to the filtering system are reported to and managed by the school business manager.

Where personal mobile devices are allowed (e.g. visitors giving presentations), internet access through the school network ensures that filtering is applied that is consistent with school practice.

FILTERING CHECKLIST

Checklist	In Place	Partially	Not in Place
The school maintains and supports the managed filtering service provided by the Internet Service Provider			
The school provides differentiated user-level filtering through the use of the Sophos filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff, pupils etc.)			
In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this is logged and carried out by a process that is agreed by the Headteacher			
Mobile devices that access the school internet connection (whether school or personal devices) are subject to the same filtering standards as other devices on the school systems			
Any filtering issues are reported immediately to the filtering provider			

Checklist	In Place	Partially	Not in Place
Requests from staff for sites to be removed from the filtered list are considered by the headteacher and school business manager. If the request is agreed, this action is recorded and logs of such actions are reviewed regularly by the LGB.			
Pupils made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.			
Staff users are made aware of the filtering systems through: ▪ the Acceptable Use Agreement ▪ induction training ▪ staff meetings, briefings, Inset.			
Parents are informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.			

MONITORING

No filtering system can guarantee 100% protection against access to unsuitable sites. Wootton-by-Woodstock School will therefore monitor the activities of users on the school network and on school equipment as indicated in the e-safety policy and the Acceptable Use Agreement. The headteacher will report this to the governors at least annually and a record of internet access and breaches of the school's filtering mechanisms included in headteacher reports.

AUDIT/REPORTING

Logs of filtering change controls and of filtering incidents are made available to

- The headteacher
- The school business manager and computing coordinator
- A named e-safety governor
- External filtering provider

The filtering section of this policy is reviewed in response to the evidence provided by the audit logs of the suitability of the current provision.

MEMORY STICKS/CDS/DVDS

Personal details of staff and pupils should not normally be stored on external devices. On the rare occasions that this is necessary, these devices should not be removed from school and should be stored in the locked key cabinet.

Documents should be removed from the memory stick at least termly.

FURTHER GUIDANCE

The following guidance is recommended:

- Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015).
- UKSIC produced guidance on / information on "Appropriate Filtering"
- NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/