Swanland
Education Trust

Policy for
Technical Security

Document Ref:	
Name and Title of Author:	Chris Huscroft – CEO
Name of Responsible Committee:	Board of Trustees
Trade Union Representative Approval:	
Implementation Date:	January 2019
Review Date:	January 2022
Version:	1
Trustee Approval Date:	
Target Audience:	
Related Documents:	Computing Policy, Online Safety Policy, Social Media Policy, Acceptable Use Policies (pupils/staff/parents), Anti-Bullying Policy (Cyber Bullying)
References:	

Revision History

Version	Date	Summary of Revision	Revision Author
1	Jan '19	Trust version created and recommended for approval	CJH

Contents

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training.

Aims:

The trust/school will be responsible for ensuring that their 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 trust's data policy;
- logs are maintained of access by users and of their actions while users of the system;
- there are regular reviews and audits of the safety and security of school computer systems.

Technical Security:

The trust/school will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- Trust/school technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of trust/school 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 trust/school systems and data;
- All users will have clearly defined access rights to school/ technical systems;
- 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;
- The technical support team engaged to support the trust/school 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
- The Head Teacher and Online Safety Leader 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;
- The trust/school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc

Passwords:

A safe and secure username and password system is essential if the above is to be established and will apply to all school technical systems, including networks and email.

- All users will have clearly defined access rights to trust/school technical systems and devices;
- The main administrator username/password for the school technical systems is known by the technical support team engaged to support the trust/school;
- All school networks and systems will be protected by secure passwords that are regularly changed;
- Staff users will change their passwords at regular intervals – every half term;
- Children will access the tablets using Kids Place;
- Children will be taught the importance of password security;
- All users (staff and children) will have responsibility 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;
- Passwords for new users, and replacement passwords for existing users will be allocated The technical support team engaged to support the trust/school;
- When away from their workstation staff should "lock" their laptop/computer, to avoid compromising the security of the trust/school network.

Filtering:

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school and the technical support team engaged to support the trust/school. Illegal content is filtered by the 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 trust/school to breaches of the filtering policy, which are then acted upon.

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 online safety and acceptable use. It is important that the trust/school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in each school.

- The responsibility for the management of the school's filtering policy will be held by the technical support team engaged to support the trust/school. They will manage the school filtering (using Smoothwall), in line with this policy and will keep records / logs of changes and of breaches of the filtering systems;

- All users have a responsibility to report immediately any infringements of the trust/school's 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;
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school 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 support team engaged to support the trust/school only. If the request is agreed, this action will be shared with the Online Safety Leader.

Monitoring:

Monitoring is needed to ensure that early intervention can be put in place for those users attempting to access filtered websites and those in breach of the Acceptable Use Agreements. Filtering and monitoring work together to safeguard the user.

- This trust uses Smoothwall Reporting Portal to monitor users' online behaviours. All users are made aware of this through the Acceptable Use Agreements;
- Daily reports of attempted access to filtered websites and/or search terms will be sent to the Headteacher and Online Safety Leader for analysis. If action is seen as necessary, the steps outlined in the Online Safety Policy will be followed;
- The Head Teacher has the right to request historic monitoring reports (prior to January 2018) **only** if they are needed in an investigation. The user/s involved will be told that this is going to happen prior to the historic reports being sought.

INSERT HERE DETAILS OF THE TECHNICAL SUPPORT COMPANY THAT MANAGES and MAINTAINS YOUR SYSTEMS