Policy Title:	**Technical Security**	
Version:	2	
Date of Issue:	Summer Term 2021	
Date of Review:	Spring Term 2023	
Author(s):	M Hodgeon	
Ratified by:	Governors Policy Committee	
Responsible signatory:	**Chair** H.McCann	**Vice Chair** W.Blundell
Amendments:	Reference to BTLS replaced, now rebranded and now known as LCC EDS. Reference to Zuludesk replaced, now rebranded and now known as JamF. Reference to ICT Manager now updated to new title Strategic Lead ICT and Digital Transformation Reference to LMT replaced with LT Reference to C Harwood SBM replaced with A Millard SBM	
Date:	June 2021	
Outcome:	This Policy: details user responsibilities for Technical Security within Astley Park School, and is designed to help them understand their position	
Cross Reference:	Acceptable Use Policy Online Safety Policy Staff iPad Agreement	

EQUALITY AND DIVERSITY STATEMENT

Astley Park School is committed to the fair treatment of all in line with the Equality Act 2010. An equality impact assessment has been completed on this policy to ensure that it can be implemented consistently regardless of any protected characteristics and all will be treated with dignity and respect.

POLICY REVIEW

To ensure that this policy is relevant and up to date, comments and suggestions for additions or amendments are sought from users of this document. To contribute towards the process of review, please contact the policy author.

Technical Security Policy (including filtering and passwords)

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 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.

Responsibilities

The management of technical security will be the responsibility of the Strategic Lead ICT and Digital Transformation in conjunction with LCC EDS/Bowker IT.

Technical Security

Policy statements

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 receive guidance and training and will be effective in carrying out their responsibilities:

- School will be managed in ways that ensure that the school meets recommended technical requirements in accordance with Local Authority and Online Safety Policy Guidance
- There will be regular reviews and audits of the safety and security of 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 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 will be recorded by the Strategic Lead ICT and Digital Transformation and will be reviewed, at least annually, by the Online Safety 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.
- The Strategic Lead ICT and Digital Transformation is 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. We have a clear mobile device policy for staff and visitors. Use of school mobile devices is monitored and filtered using LCC EDS Netsweeper and restrictions are in place using Mobile Device Management (MDM) system - JamF.
- The Strategic Lead ICT and Digital Transformation/LT regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy/Staff iPad Agreement. At Astley Park School we use Netsweeper Filter which is provided by the Local Authority/LCC EDS.
- Our ICT Tickets/CPOMS reporting systems are in place for users to report any actual / potential technical incidents to the Strategic Lead ICT and Digital Transformation.
- Anyone accessing the school systems including trainee teachers, supply teachers, and visitors digitally sign/agree to the school Acceptable Use Policy.
- Acceptable Use/Online Safety Policy/Staff iPad Agreement is in place and covers the downloading of executable files and the installation of programmes on school devices by users.

- Acceptable Use/Online Safety Policy/Staff iPad Agreement is in place and covers the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- Acceptable Use/Online Safety Policy is in place and covers the use of removable media (eg USB sticks / CDs / DVDs) by users on school devices. The school no longer allows the use of USB sticks for data storage and has implemented the use of 1TB of OneDrive cloud storage as an alternative.
- The school infrastructure and individual workstations are protected by up to date software (Sophos) to protect against malicious threats from viruses, worms, trojans etc
- Personal data cannot be sent over the internet/via email or taken off the school site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE). Where sensitive data is in use i.e CPOMS we have two factor authentication in place using the CPOMS Authenticator app.

Policy Statements

- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Strategic Lead ICT and Digital Transformation and will be reviewed, at least annually, by the Online Safety Group.
- The “master / administrator” passwords for the school systems, used by the Strategic Lead ICT and Digital Transformation staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place eg school safe. Consideration should also be given to using two factor authentication for such accounts.
- All users (adults and young people) 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 by M Hodgeon (Strategic Lead ICT and Digital Transformation) or in the case of SIMS – A Millard (SBM).

- Some systems allow for passwords to be issued through an automated process using the user's school email address. i.e CPOMS, Purple Mash
- Users will change their passwords at regular intervals – as described in the staff and pupil sections below.
- Where passwords are set / changed manually requests for password changes should be authenticated by the Strategic Lead ICT and Digital Transformation to ensure that the new password can only be passed to the genuine user.

Staff passwords:

- All staff users will be provided with a username and password by the Strategic Lead ICT and Digital Transformation/ automated process who / which will keep an up to date record of users and their usernames.
- The password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- should be changed at least every 90 days
- should not re-used for 6 months and be significantly different from previous passwords created by the same user.

Pupil passwords

- All users will be provided with a username and password by (Strategic Lead ICT and Digital Transformation / automated routine) who / which will keep an up to date record of users and their usernames.
- The complexity will be set with regards to the cognitive ability of the children.
- Pupils will be taught the importance of password security

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the Acceptable Use Agreement
- through the school's Online Safety Policy and School Technical Security Policy.

Pupils will be made aware of the school's password policy:

- in lessons
- through the Pupil Acceptable Use Policy

Audit / Monitoring / Reporting / Review

The responsible person (Strategic Lead ICT and Digital Transformation) will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ins
- Security incidents related to this policy

Filtering

Introduction

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 school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Strategic Lead ICT and Digital Transformation. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to a second responsible person Headteacher

All users have a responsibility to report immediately to Strategic Lead ICT and Digital Transformation any infringements of the 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.

Policy Statements

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 Netsweeper 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 school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by the LCC EDS/Netsweeper.
- The school has provided enhanced / differentiated user-level filtering through allowing different filtering levels for 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 must be 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) 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 Strategic Lead ICT and Digital Transformation via an ICT Ticket for consideration. The Strategic Lead ICT and Digital Transformation will consult with the Headteacher and will regularly review access.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme which the Online Safety Subject Lead will oversee. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Policy
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use/Online Safety Policy and through online safety awareness sessions / letters home / school messaging systems / blogs / Sharing our learning etc.

Changes to the Filtering System

- Users may request changes to the filtering by raising an ICT Ticket.
- The request will then be considered and there should be strong educational reasons for changes that are agreed.
- The Headteacher will be the second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records / audit of logs)

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Strategic Lead ICT and Digital Transformation who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Policy.

Monitoring will take place as follows:

- In lessons the Class Team closely monitor Pupil internet access
- Daily reports are scheduled and monitored by the DSL and Strategic Lead ICT and Digital Transformation to check any suspicious searches and web activity.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person Headteacher
- Online Safety Group
- Online Safety Governor / Governors committee
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Further Guidance

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).

The Department for Education 'Keeping Children Safe in Education' requires schools to: *"ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system"* however, schools will need to *"be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."*

In response UKSIC produced guidance on – information on "Appropriate Filtering"