



Filtering & Monitoring Policy

CHARITY POLICY & PROCEDURE

Document Revised:	March 2025
Ratified by Trustees:	March 2025
Next Review Date:	August 2026

Content

Aims

The following sections are included in this policy document:

1. Responsibilities
2. IT Security
3. Passwords
4. Internet Access
5. Education, Training and Awareness
6. Monitoring
7. Review

Filtering & Monitoring

Aims

The filtering and monitoring 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 and monitoring is only one element in a larger strategy for online safety and acceptable use. Talbot House Children's Charity ("the Charity") understand the importance of managing this policy, the associated risks and to provide preventative measures which are relevant to the Charity.

There is no set definition of 'security-related incidents', but in general it refers to any situation posing a risk of harm to your organisation (both to the physical infrastructure and to your staff and pupils). Please refer to our related policies; **Health and Safety**, **E-Safety** for more information.

This includes:

- Vandalism.
- Arson.
- Cyber-attacks.
- Serious incidents with a weapon.
- Terror attacks.

Filtering & Monitoring

1. Responsibilities

Our Trustees, Governors and Head Teacher have responsibilities under this policy.

- Our Trustees and Governors are responsible for:
 - Ensuring that the Charity has sufficient monitoring and filtering systems in place. The current Link Governor for Filtering and Monitoring is Trudy Johnson.
- The Head Teacher is responsible for:
 - Putting measures in place to reduce the risks of infiltration of the IT systems.
 - Keeping pupils and staff safe when using technology, from potential cyber-attacks.

1.2 IT Provider Responsibilities

- Our IT Provider is ITPS, they provide the Charity with all IT systems, software, hardware support and security.
- ITPS will liaise with the IT Support Assistant and inform the CEO and / or Head Teacher of any breaches or inappropriate traffic.
- Manage updates.
- Report issues with IT systems.

1.3 We use Ativion, for our Cloud-based IT Support, this offers category-based content web filtering, allowing us to control which websites users can access.

- Ativion includes over 80 content categories covering millions of domains and billions of web pages.
- The Charity can set policies to block or allow specific types of content, ensuring compliance with internal policies and / or external regulations.
- Being cloud-based, Ativion does not require on-premises hardware. This makes it easy to deploy and manage, providing protection whether users are on or off the Charity network.
- Ativion uses DNS-layer security to block malicious domains, IP addresses, and cloud applications before a connection is established.
- Ativion also includes features like:
 - Allow and block lists for specific sites.
 - SafeSearch enforcement to block explicit content in search results.
 - Flexible, location-aware enforcement to apply different policies based on user location.
- Overall, Ativion provides a comprehensive, scalable solution for web filtering and cybersecurity, leveraging the power of the cloud to protect. It is a filtering solution that is monitoring internet traffic 24 hours a day 7 days a week. The software is called ContentKeeper.
- The timeline for informing the Charity of any breach or access to inappropriate materials is less than 60 seconds.
- The filtering system is an educational filter solution that provides all the key requirements to be Keeping Children Safe in Education (KCSiE) compliant. It also provides the data for the DSL's to become proactive with the solution and not reactive.

Filtering & Monitoring

- ITPS will triage any support call to Atvion, any updates and patching will be communicated between the Charity and Atvion, however ITPS are able to support further.

2. IT Security

All users will have clearly defined access rights to the Charity's systems and devices.

- Charity networks and systems will be protected by secure passwords that are regularly changed.
- The "master / administrator" passwords for the Charity systems, used by IT Support Assistant must also be available to the CEO and / or Head Teacher and kept in a secure place. Consideration should also be given to using two factor authentications for such accounts.
- All users (staff and pupils) will have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Staff must immediately report any suspicion or evidence that there has been a breach of security.
- A log-in and email username and password for new users and replacement passwords for existing users will be issued through an automated process, initiated by the IT Support Assistant.
- Users will change their passwords at regular intervals, as described in the 'Passwords' section below.

2.1 Passwords

- Staff Passwords.
 - All staff users will be provided with a log-in and email username and password as outlined above.
 - The password should be a minimum of 8 characters long and it must include an uppercase character, a lowercase character, a number and a special character.
 - Staff should avoid using passwords with personal names or any other personal information about the user that might be known by others.
 - Temporary passwords (issued for new user accounts or when users have forgotten their passwords), shall be set to enforce a 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).
 - Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
 - Passwords should be changed as requested when logging in.
- Pupil Passwords.
 - All pupil users in school will be provided with a username and password by the IT Support Assistant, who will keep an up-to-date record of users and their usernames.
 - Users will be required to change their password every year.
 - Pupils will be taught the importance of password security.
 - The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the pupils.

Filtering & Monitoring

- Users at KS1 and below will use a generic class username and password which will enable them to access the Charity's network – including the pupil shared area.
- Users above KS1 will have a unique username and password to login in. Their class teacher must keep this safe and secure and encourage as many children as possible who can to remember it according to their need.

3. Internet Access

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the Charity, with the support of ITPS. Illegal content is filtered by the broadband or filtering provider. Filter content lists are regularly updated, and internet use is logged and frequently monitored. The monitoring process alerts the Charity to breaches of the agreed filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system.

- Personal mobile devices are not allowed internet access through the Charity network, unless authorised by the CEO and /or Head Teacher, filtering will be applied that is consistent with school practice.

3.1 The Charity maintains and supports the managed filtering service provided by the Internet Service Provider (ITPS).

- Authorised personal devices will be subject to the same filtering standards as other devices on the Charity systems.
- Any filtering issues should be reported immediately to the IT Support Assistant.
- Requests from staff for sites to be removed from the filtered list will be considered by the CEO and / or Head Teacher (if the request is agreed, this action will be recorded).

4. Education, Training and Awareness

- Staff users will be made aware of the filtering systems through:
 - The Acceptable Use of Charity Internet, ICT Systems and Equipment Agreement (Staff).
 - Induction training.
 - Further CPD / online training.
 - Staff meetings, briefings and training days.
- Pupils will be made aware of the importance of filtering systems through:
 - Teaching in our PSHE curriculum.
 - Focus days and preparation for adulthood learning.
 - Discussions of the consequences of attempting to subvert the filtering system.
 - The Acceptable Use of Charity Internet, ICT Systems and Equipment Agreement (Pupils), on admission and then annually.
- Parents will be informed of the school's filtering policy through:
 - The Acceptable Use of Charity Internet, ICT Systems and Equipment Agreement (Parents / Carers).
 - Communications including the Charity's: website, social media pages and newsletters.

Filtering & Monitoring

5. Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The Charity will therefore monitor the activities of users on the Charity network and on Charity equipment as indicated in the E-Safety Policy and the Acceptable Use of Charity Internet, ICT Systems and Equipment Agreements.

6. Review

This policy will be reviewed by the Head Teacher, who will make any changes necessary, and will communicate changes to all members of staff.

Filtering & Monitoring



I have read, understood, and acknowledge this policy and will endeavour to follow the guidance outlined within.

Print Name: _____

Job Title: _____

Signature: _____

Date: _____

Please complete full details above, once complete please return to the HR Department within 5 working days.

Please do not hesitate to contact me should you have any questions.

HR Department

Talbot House Children's Charity