Thornleigh
Salesian College

Filtering and Monitoring Policy

Person Responsible:	AAHT Whole School ICT
Last Reviewed:	January 2024
Adopted:	January 2024
Next Review due:	January 2026

1. 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 aim of the filtering and monitoring system at Thornleigh Salesian College aims to ensure that all students and staff are safe when using the internet and technology in school; without over blocking websites to allow access to educational resources and does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding

Filtering refers to the categorisation of websites and technology including which websites are accessible from school. Monitoring is the day-to-day tracking of users' access to different websites. At Thornleigh Salesian College we use Sophus for filtering and Net-Support for Monitoring internet access.

With changes in technology and new websites the filtering system cannot provide a 100% guarantee that all information will be appropriately filtered. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation at Thornleigh Salesian College. The following information with documentation and responses from Sophus and UK Safer Internet Centre references how this is provided. The filtering checking procedure is also documented in this policy.

The DSL along with our Associate Assistant Headteacher for IT and the Network Manager are responsible for ensuring that:
- The service is maintained and accessible for all school sites to use
- All relevant safeguards are being met
- School is taking necessary precautions to ensure the service provided is appropriate
- Provide investigation of any web filtering related issues including:
    - Access to websites containing inappropriate or potentially harmful material
    - Access to websites containing educational or related material deemed appropriate for school
- Provide web access reports

The schools filtering software is Sophus and they have worked to ensure that the UK Safer Internet Centre checklist is followed. As a school we then use this guidance and tailor it to our local context. Sophus web filtering service meets and exceeds the Ofsted guidelines. The filtering solution is constantly updated via national feeds from the wider Internet community to ensure that as new websites are created they are categorised and sanctioned accordingly. Sophus also provides the following features:
- Application Control – this stops some applications running which utilise peer to peer (file-sharing) features
- Intrusion Prevention – this is aimed at stopping hackers from gaining access to our endpoints
- Website Certificate Inspection – this checks websites to ensure any certificates are valid and up to date. This stops users accessing malicious websites or websites that are not properly maintained.

Schools in England 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) Furthermore, it expects that they “assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology”. Department for Education’s statutory guidance ‘Keeping Children Safe in Education’ obliges schools and colleges in England 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.” This policy sets out to outline how we are appropriately “Meeting digital and technology standards in schools and colleges” DFE 23 March 2022 (Updated 29th March 2023)

The schools monitoring software is Net Support. Netsupport DNA uses a database of pre-supplied safeguarding keywords and phrases covering topics from self-harm, bullying and racism through to risks of radicalisation. NetSupport DNA monitors the school network and uses advanced neurolinguistics to capture triggered keywords used anywhere on the network, while ensuring accurate detection and avoiding false alarms. Trending safeguarding terms are also highlighted in the student-generated word cloud in classroom.cloud, so teachers are aware of what students are typing or discussing.

NetSupport DNA's triggered events provide Head of Years with an insight into students struggling with any type of safeguarding issue or inappropriate searches. Teachers can also mark any students they are particularly concerned about as 'vulnerable' on the system.

From the information provided to us by our supplier Sophus, we are confident that the web filtering solution as configured meets the current DfE guidance.

2. Roles and Responsibilities

The responsibility for the management of the school's filtering and monitoring policy will be ultimately held by the headteacher and the DSL supported by the Associate Assistant Headteacher for IT and the Network Manager. This currently includes:
Headteacher: Andrea O'Callaghan
Designated Safeguarding Lead: Charlotte Sharp
Associate Assistant Headteacher for IT: Chris Atkinson
Network Manager: Brad Shaw
Governor: Anne-Maria Parkinson

Their responsibility is to uphold the standards set out in this policy for the filtering and monitoring of data at Thornleigh Salesian College. They will manage the school filtering, in line with this policy; keeping records of the different categories blocked for all users (staff and students) and will keep records/logs of changes and of breaches of the filtering systems.
To ensure that there is a system of checks and to protect those responsible, changes to the schools filtering service must:
• be logged in the filtering categorisation document (Appendix 1)
• be reported to the Headteacher
• testing the filtering system termly

All users of the school network at Thornleigh Salesian College have a responsibility to report immediately to the DSL 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.

Heads of year are responsible for reviewing filtering logs and taking appropriate action; reporting to the DSL any concerns and recording on CPOMS and ClassCharts.

3. Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the Digital Safety and Wellbeing program at KS3, KS4 and KS5. At KS3 this will take place during computer science lessons and KS4 and KS5 during the tutor time programme. 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:
• signing the AUP
• induction training
• Digital Safety and Wellbeing termly updates.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement when students join the school.

4. Review of the Filtering and Monitoring Provision & Changes to the Filtering System

4.1 Categorisation of Websites

4.1.1 Websites will be automatically categorised by out filtering software “Sophus”. Sophus work to ensure that the UK Safer Internet Centre checklist is followed. Sophus web filtering service meets and exceeds the Ofsted guidelines. The filtering solution is constantly updated via national feeds from the wider Internet community to ensure that as new websites are created they are categorised and sanctioned accordingly. Sophus also provides the following features. The different categories that Thornleigh Salesian College have decided to block / allow access to can be found in appendix A.

4.1.2 Thornleigh Salesian College have then made decisions regarding the categories that we allow staff and students to access (Different user access levels for staff and students). Ensuring that all students and staff are safe when using the internet and technology in school; without over blocking websites to allow access to educational resources and does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

4.1.3 Staff can request a website is to be “whitelisted” (unblocked) by emailing the network manager and Associate Assistant Headteacher for IT. The Associate Assistant Headteacher for IT will lease with the DSL to agree to whitelist the website. If it is felt that the site should be unfiltered the Network Manager will make the appropriate change within Sophus.

4.1.4 Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered should report this in the first instance to the DSL or the Associate Assistant Headteacher for IT who will decide whether to make school level changes (as above). If it is felt that the site should be filtered the Network Manager will make this change within Sophus.

4.1.5 The network manager will conduct a termly test of the filtering system to ensure that the appropriate Sophus filters are working for staff and students and make changes to the Sophus settings should a concern arise.

4.1.6 The filtering categories will be reviewed annually and changes recorded in appendix A; following the statement for changes listed in 4.1.2

4.1.7 Netsupport monitoring logs will be used to support the decisions on filtering; reviewing current trends for student searches and will impact the filtering decisions.

4.1.8 Automatic notifications alert the DSL of common searches for students in key categories and these are listed in appendix A. Any concerns will be recorded within CPOMS as defined in the “POLICY”

5. Updates to this Policy

5.1 Updates to this Policy

5.1.1 In light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available. This policy will be reviewed every two years.

Student ICT Agreement – AUP supplemental

Students are permitted to use Thornleigh Salesian College ICT Facilities after agreeing to the following conditions:

1. I will use school ICT facilities, including the internet, e-mail, digital video, mobile devices, 3rd party services, virtual learning environment (Google Classroom) etc. for school purposes only.

2. I will not download or attempt to install software on school ICT Facilities.

3. I will only access the school network and 3rd party services using my own username and password supplied to me by the school.

4. I will follow the school's ICT Acceptable Use Policy and not reveal my passwords to anyone and change them regularly.

5. I will make sure that all ICT communications with other students, teachers or others are responsible and sensible.

6. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.

7. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

8. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring them into disrepute.

9. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community

10. I will respect the privacy and ownership of others' work on-line at all times.

11. I will not attempt to bypass the school internet filtering system in any way, regardless of what device I am using.

12. I understand that all my use of school ICT Facilities including Internet access and other related technologies is monitored and logged and can be made available on request to teachers.

13. I understand that these rules are designed to keep me safe and that if they are not followed, college sanctions will be applied and my parent/carer will be contacted.

14. I will not attempt to cause damage to the school infrastructure.

15. I will not attempt cyber-attacks.

Signature _____

Printed Name _____

Date _____

Guest and Staff ICT Agreement – AUP supplemental

Guests are permitted to use Thornleigh Salesian College ICT Facilities using the guest WIFI after agreeing to the following conditions:

1. I understand that I'm personally accountable for what I do online with school technology or using the school WIFI and infrastructure.

I will use school ICT facilities, including the internet, e-mail, digital video, mobile devices, 3rd party services, virtual learning environment (Google Classroom) etc. for school purposes only.

2. I will not download or attempt to install software on school ICT Facilities.

3. I will only access the school network and 3rd party services using my own username and password if supplied to me by the school.

4. I will follow the school's ICT Acceptable Use Policy and not reveal my passwords to anyone and change them regularly.

5. I will make sure that all ICT communications with other students, teachers or others are professional.

6. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of the senior leadership team.

7. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring them into disrepute.

8. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community

9. I will respect the privacy and ownership of others' work on-line at all times.

10. I will not attempt to bypass the school internet filtering system in any way, regardless of what device I am using.

11. I understand that all my use of school ICT Facilities including Internet access and other related technologies is monitored and logged and can be made available on request.

12. I will not attempt to cause damage to the school infrastructure.

13. I will not attempt cyber-attacks.

14. I will only use the information, systems and equipment in line with our security and information management policies.

15. I will report any breach of this AUP to a member of the Senior Leadership Team

16. I am aware that I can use the 'Whistleblowing Policy', and raise a concern if it's believed that someone is misusing our information and technology.

17. I will ensure that computer devices connected to the school systems are locked / logged out of when not in use.

18. I understand that I have a legal responsibility to protect personal and sensitive information and adhere to the GDPR policy; social media policy; staff conduct policy.

19. I will not provide information in response to callers or emails whose identity I cannot verify.

Signature _____

Printed Name _____

Date _____