

Telford & Wrekin IDT Managed Services



Education & Skills
Funding Agency

Academy trust guide to cyber crime and cyber security

Telford and Wrekin IDT Services Response
October 2022



Services
for schools



www.twccommercial.co.uk

servicesforschools@telford.gov.uk

01952 380522

Contact us to discuss your requirements

Introduction

- Kirsty King - IDT Service Delivery Manager
- Presentation content provided by :
 Andy Carpendale – IDT Security Specialist

ESFA Checklist

Cyber crime: what can trusts do?

- To comply with the requirements of the Academies Financial Handbook (paragraph 4.8.1) and address the risk of fraud, theft and/or irregularity, trusts should as a minimum:
- use firewalls, antivirus software and strong passwords
- routinely back up data and restrict devices that are used to access data
- train staff to ensure that they:
 - check the sender of an email is genuine before, for example, sending payment, data or passwords
 - make direct contact with the sender (without using the reply function) where the email requests a payment
 - understand the risks of using public wifi
 - understand the risks of not following payment checks and measures

ESFA Checklist

Cyber crime: what do Telford and Wrekin IDT Services provide:

- Boundary firewall protection with internet filtering and proxy technology that protects machines from direct connectivity to the Internet.
- Antivirus protection is installed on all machines and updates every 2 hours. Any portable media is scanned when attached
- Deploy fine grained password policies which schools can use to set strong passwords, we also use a user creation toolkit so the password reset process can be delegated to the school.
- A backup solution that is hosted in the IDT Services datacentre. Backups run every morning and evening, with the SIMS database every 4 hours. Retention period is currently 90 days.
- As part of our investment in office365, multifactor authentication is available to provide extra security around logins into the office365 service.

ESFA Checklist

Cyber crime: what do Telford and Wrekin IDT Services provide:

- Regular email reminders about SPAM and Phishing Attacks and what you should do guidance.
- We can provide specific training on request.
 - Schools and Trusts procure Audit and Scrutiny advise through a number of different suppliers and we can support this.

ESFA Checklist – 5 Strategic Questions

1. Information Held

Does the trust have a clear and common understanding of the range of information assets it holds and those that are critical to the business?

We are able to help assist with audits.

ESFA Checklist – 5 Strategic Questions

2. Threats

Does the trust have a clear understanding of cyber threats and vulnerabilities?

Are you aware? Risks of sharing data over personal accounts, storage of any data, password security?

National Cyber Security Centre – Board Toolkit

Resources designed to encourage essential cyber security discussions between the Board and their technical experts.

<https://www.ncsc.gov.uk/collection/board-toolkit>

ESFA Checklist – 5 Strategic Questions

3. Risk management

Is the trust proactively managing cyber risks as an integrated facet of broader risk management including scrutiny of security policies, technical activity, user education and testing and monitoring regimes against an agreed risk appetite?

Automated internal vulnerability assessments are completed on a weekly basis and externally on a bi-monthly basis by an approved 3rd party.

Logging of privileged user activity, permission changes and access.

User awareness training around security themes is available on request

ESFA Checklist – 5 Strategic Questions

4. Aspects of risk

Does the trust have a balanced approach to managing cyber risk that considers people (culture, behaviours and skills), process, technology and governance to ensure a flexible and resilient cyber security response?

We maintain an IDT Risk Register which feeds into the Council's corporate risk register where the risk score is deemed as high.

Solutions and services will be risk managed as part of the project delivery mechanism or as part of the procurement process.

We report to a quarterly Governance Board chaired by Head Teachers on performance and any Cyber Security concerns.

ESFA Checklist – 5 Strategic Questions

5. Governance oversight

Does the trust have sound governance processes in place to ensure that actions to mitigate threats and maximise opportunities in the cyber environment are effective?

Report to a quarterly Governance Board chaired by Head Teachers on performance and any Cyber Security concerns.

Operate a change management board weekly.

Representation on the Council Security Group.

ESFA Checklist – 10 Steps

1. Home and mobile working

- A secure baseline build which can include encryption is applied to all equipment, delivered as part of our deployment process and this is the same deployment method for monthly security patches.
- We provide data in transit security as part of the remote access solution, Schools can also request bit locker for devices for data at rest protection as part of our bit locker encryption offering. Email encryption is also available.

ESFA Checklist – 10 Steps

2. User education and awareness

- User awareness training around security themes is available on request.
- Regular email reminders about SPAM and Phishing Attacks and what you should do.
- Issues and incidents can be reported via the IDT Self Service or if this is a priority 1 incident via Telephone (where appropriate)

ESFA Checklist – 10 Steps

3. Incident management

- We use ITIL Incident and Problem Management processes, in a major incident we will invoke an Emergency Response Team which will link into the council resilience team as appropriate.
- Disaster recovery capability through backup solution.
- IDT Services will work with or report to Schools SMT, Council Audit, internal Human Resources departments and law enforcement when required to do so.

ESFA Checklist – 10 Steps

4. Information risk management regime

- Update an IDT Risk Register which feeds into the Council's corporate risk register where the risk score is deemed as high.
- We will report risks to Head Teachers within schools and to the Governance Board.
- IDT have membership of the National Cyber Security Centre's Cyber Information Sharing partnership to discuss and to gather intelligence relating to cyber security threats.

ESFA Checklist – 10 Steps

5. Managing user privileges

- Provide a user management toolkit for key staff within school and reporting is also available on request.
- Privileged accounts are monitored and restricted to permitted personnel only.
- Monitor and control access to log data, IDT use log analytical technology to monitor for unusual behaviour.

ESFA Checklist – 10 Steps

6. Removable media controls

- Provide an endpoint/device antivirus solution to enable staff to scan removable media.

ESFA Checklist – 10 Steps

7. Monitoring

- We have monitoring solutions and capabilities in place across our systems and networks. Ranging from reliability monitoring to threat monitoring allowing the ability to detect unusual activity.
- We use a product called Senso to enable schools to monitor usage. Designed with the UK Government Prevent duty, UK Safer Internet Centre, the UK Department for Education's Keeping Children Safe in Education (KCSiE) guidance and with keyword and URL lists from the Internet Watch Foundation(IWF) aids schools in fulfilling their legal duty of care around online safety and safeguarding.

ESFA Checklist – 10 Steps

8. Secure configuration

- Can assist with completion of a system inventory which will list the information on machines that you have joined to your network.
- Provide a secure defined baseline build which is delivered as part of a deployment process, this is the same deployment method for monthly security patches.
- Complete monthly patching in line with the IDT Services Patch Management Policy.

ESFA Checklist – 10 Steps

9. Malware protection

- Provide antivirus and anti-malware protection on endpoints/devices, email and internet filtering, with a combination of on access and scheduled scanning in place.
- Restrictions are in place for staff and students to prevent unauthorised software installations.

ESFA Checklist – 10 Steps

10. Network security

- Manage the network perimeter including boundary or client side Firewalls.
- We manage and control access to our own datacentres, IDT can assist in reporting on high risk assets on request.
- Complete automated internal vulnerability assessments on a weekly basis and external testing is completed on a bi-monthly basis by an approved 3rd party.

Telford & Wrekin IDT Managed Services



Education & Skills
Funding Agency

Keeping Children Safe in Education Filtering and Monitoring

Telford and Wrekin IDT Services Response October 2022



www.twccommercial.co.uk

servicesforschools@telford.gov.uk

01952 380522

Services
for schools

Contact us to discuss your requirements

Filtering and Monitoring

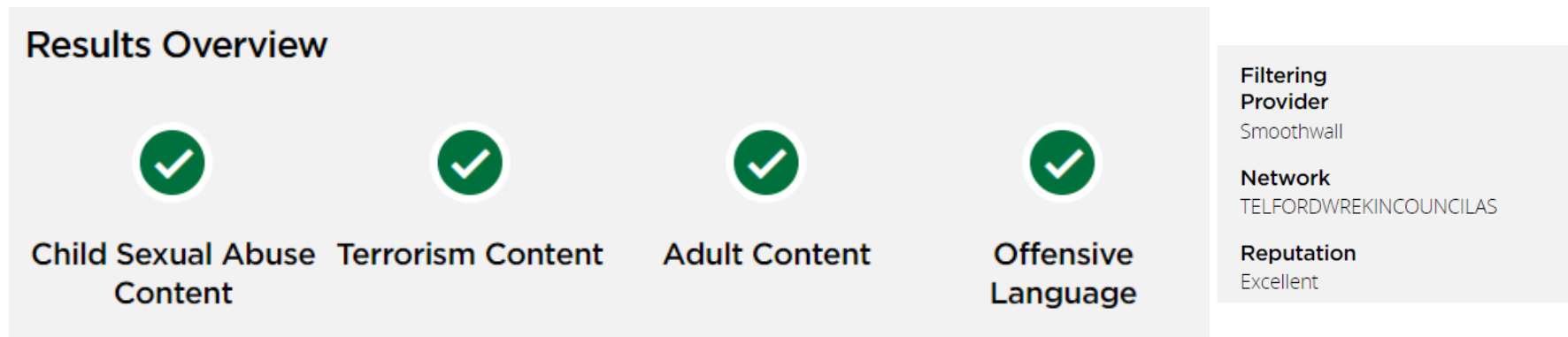
- Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system.
- As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness

How do IDT meet this requirement?

- Internet Filtering Provision: Smoothwall

smoothwall®

- This blocks access to any of the material listed below
- Using the DfE recommended testing site by SWGfL here are the results:-



How do IDT meet this requirement?

Child Sexual Abuse Content



Blocked

Description

Tests whether you are blocking websites on the IWF Child Abuse Content URL list.

Results & Recommendations

It appears that your filtering solution includes the IWF URL Filter list, blocking access to Child Sexual Abuse content online

Terrorism Content



Blocked

Description

Tests whether you are blocking websites on the Counter-Terrorism Internet Referral Unit list (CTIRU).

Results & Recommendations

It appears that your filtering solution includes the Counter-Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online

Adult Content



Blocked

Description

Test whether your Internet filter blocks access to pornography websites

Results & Recommendations

It appears that your filtering solution includes blocking for online pornography

Offensive Language



Blocked

Description




Accesses a page containing offensive language to test if your filtering software blocks it

Results & Recommendations

It appears that your filtering solution includes blocking for offensive language





UK Safer Internet Checklist

Illegal Online Content

Aspect	Rating	Explanation
Are IWF members		Yes, Smoothwall is a member of the Internet Watch Foundation and implements the IWF CAIC list
and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Smoothwall implements the IWF CAIC list of domains and URLs. Smoothwall Filter also uses a number of search terms and phrases provided by IWF and their members. We perform self certification tests daily to ensure that IWF content is always blocked through a Smoothwall Filter
Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Smoothwall Filter implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office






UK Safer Internet Checklist

Inappropriate Online Content

Aspect	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		The 'Intolerance' category covers any sites which promote racial hatred, homophobia or persecution of minorities. Sites which advocate violence against these groups are also covered by the Violence category.
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances		The Drugs category covers the sale, manufacture, promotion or use of recreational drugs as well as abuse of prescription drugs. Sites which provide resources which aim to help those suffering from substance abuse are covered by the 'Medical Information' category. Sites which discuss Alcohol or Tobacco are covered by the 'Alcohol and Tobacco' category.
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance		The 'Terrorism' category contains the 'police assessed list of unlawful terrorist content'. Smoothwall also provides both a 'Violence' category which covers violence against both animals or people; An 'Intolerance' category (covered further above) and a 'Gore' category which covers any sites which describe or display gory images and video.
Malware / Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		As well as providing a level of protection against externally created malware, Smoothwall Filter provides a Hacking category which includes sites such as "how to" on hacking, and sites encouraging malicious computer use. Filter bypass tools are covered separately in a comprehensive "web proxies" category, which uses a combination of domain lists and dynamic content analysis.

UK Safer Internet Checklist

Inappropriate Online Content

Aspect	Explanatory notes – Content that:	Rating	Explanation
Piracy and copyright theft	Includes illegal provision of copyrighted material		The 'Piracy and Copyright Infringement' category contains sites which illegally provide copyright material or provide peer-to-peer software.
Self Harm	Promotes or displays deliberate self harm (including suicide and eating disorders)		The 'Self Harm' category contains sites relating to self-harm ,suicide and eating disorders. The category excludes sites which aim to provide medical or charitable assistance which are categorised as 'Medical Information' or 'Charity and Non-Profit' respectively
Violence	Displays or promotes the use of physical force intended to hurt or kill		The 'Violence' category contains sites which advocate violence against people and animals. We also provide a 'Gore' category which contains images and video of gory content
Pornography	Display ssexual acts or explicit images		The 'Pornography' category contains sites containing pornographic images, videos and text. Sites which contain mild nudity for purposes other than sexual arousal are covered by the 'Non-Pornographic Nudity' category. The 'Pornography' category uses both a list of domains/URLs as well as dynamic content rules which ensure new, previously unseen sites can be identified on the fly.
Multiple language support – the ability for the system to manage relevant languages			Smoothwall's combined blocklist include words in a wide variety of languages, focussed on those spoken in UK and US schools. This includes Polish and Spanish as well as "non latin" such as Urdu and Russian.

How to IDT meet this requirement?




- Classroom Monitoring Provision: Senso



- More than 99% active web coverage and accuracy
Web traffic from 600+ million end users globally. Over 200 languages supported Daily and real-time updates. Senso's filter cloud not only benefits from extensive category-based libraries to block inappropriate websites, but also uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries









UK Safer Internet Checklist

Illegal Online Content

Aspect	Rating	Explanation
Are IWF members		Senso® is a member of the IWF and actively communicate with them.
and block access to illegal Child Abuse Images(by actively implementing the IWF URL list)		IWF Lists are provided updated within Senso via an API
Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		CTIRU URL Lists are provided and updated in real time within Senso via an API

UK Safer Internet Checklist

Inappropriate Online Content

Aspect	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		Discrimination Category is one of 500 + unique content categories, and includes daily and real-time updates, as well as ActiveWeb traffic from over 600+ million end users globally with 99% ActiveWeb Coverage and Accuracy
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances		Several categories combine to cover Drugs & Substance Abuse Categories as above
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance		Extremism category as above plus Daily updates of the CTIRU URL lists
Malware / Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Yes – covered within Malicious Internet Activity Category
Pornography	Display ssexual acts or explicit images		Adult Content Category included as above
Piracy and copyright theft	Includes illegal provision of copyrighted material		Covered within Criminal Activity / Piracy Category
Self Harm	Promotes or displays deliberate self harm (including suicide and eating disorders)		Self Harm Category included as above
Violence	Displays or promotes the use of physical force intended to hurt or kill		Weapons / Violence category included as above

How to IDT meet this requirement?

- Senso Safeguard Cloud :
- Cloud based, real time monitoring of activity on school owned devices, designed to highlight to school staff users who may be vulnerable or at risk to themselves, at risk to others or behaving inappropriately. Senso indicates a potential concern by raising a “violation” when a keyword, acronym or phrase typed, matches against those found within our libraries.
- The violation information including a screenshot can then be viewed in the dashboard by the relevant Senso Safeguarding Portal User. The screenshot will also be analysed by our AI driven image analysis to indicate whether a student is potentially viewing harmful or inappropriate content alongside the keyword typed. This helps with prioritisation of Senso violations.
- Integrates with CPOMS & Myconcern - If your school would like this integration please log a call on the IDT portal or speak to your IDT Gold Technician.

