CHARTERHOUSE

IT Online Technical Security Policy

Author: A Kempster | **Lead:** A Kempster | **Last reviewed**: Aug 2026 | **Next Review**: August 2027

DEFINITION OF THIS POLICY

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. This is informed by the Department for Education (DfE) guidance, Keeping Children Safe in Education, and the Digital and Technology Standards and therefore applicable for schools and colleges in England. The school is responsible for ensuring that the 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
- access to personal data is securely controlled in line with the school's data protection and records retention policy
- system logs are maintained and reviewed to monitor user activity
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems, including filtering and monitoring provision

Responsibilities

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. The management of technical security is the responsibility of Governors and Senior Leaders, supported in this by the Designated Safeguarding Lead, Online Safety Lead and IT Department.

Technical information within this document should not be shared to anyone outside the Charterhouse group of schools.

Policy statements

The school is 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. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- **school technical systems will be managed in ways that ensure that the school meets recommended industry best practices.**
- **school IT purchases will be managed in accordance with the IT Purchasing Policy for staff, including all online software or AI based tools and services in accordance with safeguarding, data protection and cybersecurity guidelines provided by the Department of Education.**
- **cyber security is included in the school risk register.**
- **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.**
- **there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud**
- **appropriate security measures (including updates) are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data, including operating systems.**
- **the school's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.**
- **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 and accounts are deleted when the user leaves.**
- **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 IT Department, in partnership with Governors/SLT/DSL, regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.**
- **mobile device security and management procedures are in place.**
- **an appropriate system is in place, TOPdesk helpdesk system for users to report any actual/potential technical incident to the IT Support Team, who in turn will report to the SLT/DSL/Online Safety Lead (OSL).**
- **The IT Department 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.**
- **remote management tools are used by staff to monitor pupil devices in lessons**
- **guest users are provided with appropriate access to school systems based on an identified risk profile.**
- **by default, users do not have administrator access to any school-owned device.**
- **users are encouraged not to use school resources for personal matters.**
- **users are encouraged to share documents via secure link rather than as email attachments.**
- **personal data cannot be sent over the internet 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 learning platform).

Policy Statements:

- **The password policy and procedures reflect NCSC and DfE advice/guidance.**
- **Security measures are in place to reduce brute-force attacks and common passwords are blocked.**
- **School networks and systems will be protected by secure passwords.**
- **The use of passwords is reduced whenever possible, for example, using Multi-Factor Authentication (MFA).**
- **Passwords are encrypted by the system to prevent theft.**
- **Passwords have a long expiry date (100 days) and the use of password managers is encouraged.**
- **Users are able to reset their password themselves.**
- **Passwords are immediately changed in the event of a suspected or confirmed compromise.**
- **No default passwords are in use. All passwords provided "out of the box" are changed to a unique password by the IT Department.**
- **Where possible systems with access to sensitive or personal data are protected by MFA.**
- **All users 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 must not be shared with anyone.**

Filtering and Monitoring

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, as online content 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. The schools filtering system is operational, up to date, and applied to all users:

- **users, including guest accounts.**
- **school owned devices**
- **devices using the school broadband connection.**

The school filtering system is a member of the Internet Watch Foundation (IWF). The web-filtering element has a feed which incorporates 'the police assessed list of unlawful terrorist content' produced on behalf of the Home Office.

The school's filtering system:

- **filters all internet feeds, including any backup connections.**
- **filters staff, pupils and guests appropriately and it is suitable for use in an educational setting.**
- **handles multilingual web content, images, common misspellings and abbreviations.**
- **Identifies and mitigates against known technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and blocks them.**
- **provides reports when any web content has been blocked or hits a reportable category.**
- **uses content inspection (DPI) to inspect internet activity for both staff and pupils.**

Mobile and app content is often presented in a different way to web browser content; The schools firewall provides filtering on applications to mitigate the risk of harm.

Introduction to Monitoring

The schools monitoring strategy is informed by regular filtering and monitoring reviews. The schools monitoring system:

- **Sends real time alerts for certain categories of keyword searches i.e., self-harm.**
- **Involves physical supervision by staff, both in person in lessons and by means of an appropriate mobile device management system.**
- **network monitoring, using log files of internet traffic and web access using appropriate software.**

Filtering and Monitoring Responsibilities

DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Mrs Sarah Hartnell- Governor Mrs Helen Goatley - Governor
Senior Leadership	Team Member Responsible for ensuring these standards are met and:	Phil Grainge – Chief Operating Officer

	• procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	Alex Colcough - DSL
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	Anna Kempster – Director of IT
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:	• they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material	

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 by actively employing the Internet Watch Foundation (IWF) URL 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.

- **There is a filtering and monitoring system in place that safeguards staff and pupils by blocking harmful, illegal and inappropriate content.**

- **There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.**
- **Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.**
- **The filtering and monitoring provision is reviewed at least annually and checked regularly.**
- **There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.**
- **Mobile devices that access the school's internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.**

Filtering and Monitoring Review and Checks

To understand and evaluate the changing needs and potential risks of the school, the filtering and monitoring provision will be reviewed at least annually. The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the Director of IT. Additional checks to filtering and monitoring will be informed by the review process so that governors have assurance that systems are working effectively and meeting safeguarding obligations.

Reviewing the filtering and monitoring provision

A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of pupils and staff.

The review will take account of:

- **the risk profile of pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL).**
- **what the filtering system currently blocks or allows and why.**
- **any outside safeguarding influences, such as county lines.**
- **any relevant safeguarding reports.**
- **the digital resilience of learners.**
- **teaching requirements, for example, the RHSE and PSHE curriculum.**
- **the specific use of chosen technologies, including Bring Your Own Device (BYOD).**
- **what related safeguarding or technology policies are in place.**
- **what checks are currently taking place and how resulting actions are handled.**

To make the filtering and monitoring provision effective, the review will inform:

- **related safeguarding or technology policies and procedures.**
- **roles and responsibilities.**
- **training of staff.**
- **curriculum and learning opportunities.**
- **procurement decisions.**
- **how often and what is checked.**
- **monitoring strategies.**

The review will be carried out as a minimum annually, or when:

- **a safeguarding risk is identified.**
- **there is a change in working practice, e.g. remote access or BYOD.**
- **new technology is introduced.**

Checking the filtering and monitoring systems

Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked this should include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on a range of:

- **school owned devices and services, including those used off site.**
- **geographical areas across the site.**
- **user groups, for example, teachers, pupils and guests.**

Logs of checks are kept so they can be reviewed. These record:

- **when the checks took place.**
- **who did the check.**
- **what was tested or checked.**
- **resulting actions.**

Training/Awareness:

Several key staff, including the Director of IT, have attended online safety courses including CEOP and NSPCC 'Keeping Children Safe online'. Short briefing sessions for beaks and support staff are run on a regular basis to ensure that they are aware of the most up to date information.

Audit/Monitoring/Reporting/Review:
Governors/SLT/DSL/OSL will ensure that full records are kept of:

- **Training provided.**
- **Security incidents related to this policy.**
- **Annual online safety reviews including filtering and monitoring.**
- **Changes to the filtering system.**
- **Checks on the filtering and monitoring systems.**

APPENDIX A: FIREWALL CATEGORIES FOR PUPILS

Categories highlighted in yellow are blocked at all times in compliance with the UK Safer internet Centre list.
Categories not highlighted are available at all times, although there are some websites which fall within the unblocked categories that are also blocked. For a list of these websites, please contact the IT Department.

Abortion

Parent category that contains abortion-related categories.

- Abortion: Sites with neutral or balanced presentation of the issue.
- Pro-Choice: Sites that provide information about or are sponsored by organizations that support legal abortion or that offer support or encouragement to those seeking the procedure.
- Pro-Life: Sites that provide information about or are sponsored by organizations that oppose legal abortion or that seek increased restriction of abortion.

Adult Material

Parent category that contains adult-oriented categories; may also contain age-restricted content.

- Adult Content: Sites that display full or partial nudity in a sexual context, but not sexual activity; erotica; sexual paraphernalia; sex-oriented businesses including clubs, nightclubs, escort services; and sites supporting the online purchase of such goods and services.
- Lingerie and Swimsuit: Sites that offer images of models in lingerie or swimsuits, including lingerie or swimwear for sale.
- Nudity: Sites that offer depictions of nude or seminude human forms.
- Sex: Sites that depict or graphically describe sexual acts or activity, including exhibitionism; sites offering direct links to such sites.
- Sex Education: Sites that offer educational information about sex and sexuality.

Bandwidth

Parent category that contains categories known to consume bandwidth resources.

- Educational Video: Sites that host videos with academic or instructional content.
- Entertainment Video: Sites that host videos with entertainment-oriented content.
- Internet Radio and TV: Sites that provide online radio or television programming.
- Internet Telephony: Sites that enable users to make phone calls through the Internet or to obtain information or software for that purpose.
- Peer-to-Peer File Sharing: Sites that provide client software to enable peer-to-peer file sharing and transfer.
- Personal Network Storage and Backup: Sites that store personal files on web servers for backup or exchange.
- Streaming Media: Sites that enable streaming of media content.
- Surveillance: Sites that enable real-time monitoring of various operations through network cameras, webcams and other video recording devices.
- Viral Video: Sites that host videos with high or rapidly rising popularity.

Business and Economy

Parent category that contains categories related to business and economy.

- Business and Economy: Sites sponsored by or devoted to business firms, business associations, industry groups or general business.
- Financial Data and Services: Sites that offer investment advice and news and quotations on stocks, bonds and other investment vehicles, but not online trading. Includes banks, credit unions, credit cards, and insurance.
- Hosted Business Applications: Sites that provide access to business-oriented web applications and allow storage of sensitive data, excluding those for web collaboration.

Collaboration – Office

Parent category that contains the following categories:

- Collaboration - Office: Category used to manage the Office domain.
- Office - Apps: Office function that enables a user to collaborate through various applications.
- Office - Documents: Office function that enables a user to collaborate through document applications.
- Office - Drive: Office function that enables a user to collaborate through virtual storage.
- Office - Mail: Office function that enables a user to collaborate through email and messaging.

Drugs

Parent category that contains categories related to legal and illegal drugs and supplements.

- Abused Drugs: Sites that promote or provide information about the use of prohibited drugs, except marijuana, or the abuse or unsanctioned use of controlled or regulated drugs; also, paraphernalia associated with such use or abuse.
- Marijuana: Sites that provide information about or promote the cultivation, preparation or use of marijuana.
- Nutrition: Sites that provide information about nutrition.
- Prescribed Medications: Sites that provide information about approved drugs and their medical use.

Education

Parent category that contains categories of relevance to education.

- Cultural Institutions: Sites sponsored by museums, galleries, theatres, libraries and similar institutions.
- Educational Institutions: Sites sponsored by schools and other educational facilities, by non-academic research institutions, or that relate to educational events and activities.
- Educational Materials: Sites that provide information about or that sell or provide curriculum materials or direct instruction; also, learned journals and similar publications.
- Reference Materials: Sites that offer reference-shelf content such as atlases, dictionaries, encyclopedias, formularies, white and yellow pages, and public statistical data.

Entertainment

Parent category that contains entertainment-related categories.

- Entertainment: Sites that provide information about or promote motion pictures, non-news radio and television, books, humor and magazines.
- Media File Download: Sites that enable download of media content.

Extended Protection

Parent category that contains categories inferred to have potential security implications.

- Dynamic DNS: Sites that mask their identity using Dynamic DNS services, often associated with advanced persistent threats (APTs).
- Elevated Exposure: Sites that camouflage their true nature or that include elements suggesting latent malicious intent.
- Emerging Exploits: Sites found to be hosting known and potential exploit code.
- Newly Registered Websites: Sites whose domain name was registered recently.
- Suspicious Content: Sites found to contain suspicious content.

Government

Parent category that contains categories related to the government, political organizations, and the military.

- Government: Sites sponsored by branches, bureaus or agencies of any level of government, except for the armed forces.
- Military: Sites sponsored by branches or agencies of the armed services.
- Political Organizations: Sites sponsored by or providing information about political parties and interest groups focused on elections or legislation.

Human Interests

Parent category that contains categories related to human interests.

- Alcohol and Tobacco: Sites that provide information about, promote or support the sale of alcoholic beverages or tobacco products or associated paraphernalia.
- Blogs and Personal Sites: Sites that host blogs and personal sites.
- LGBTQIA+: Sites that provide information about lesbian, gay, bisexual, transgender, queer, intersex, non-binary or asexual topics, but excluding those with adult content.
- Hobbies: Sites that provide information about or promote private and largely sedentary pastimes, but not electronic, video, or online games.
- Human Interests: Sites that provide information about matters of daily life, excluding entertainment, health, hobbies, jobs, sex and sports.
- Personals and Dating: Sites that assist users in establishing interpersonal relationships, excluding those intended to arrange for sexual encounters.
- Restaurants and Dining: Sites that list, review, advertise or promote food, dining or catering services.
- Social Networking: Sites of web communities that provide users with means for expression and interaction.

Information Technology

Parent category that contains categories related to information technology.

- Computer Security: Sites that provide information about or free downloadable tools for computer security.
- Generative AI - Conversation: Sites that specialize in machine-generated conversational content for the purpose of general information, user assistance or entertainment. Includes sites hosting virtual agents and narrow domain conversational applications using AI with ability to generate new content.
- Generative AI - Multimedia: Sites that specialize in machine-generated multimedia content such as images, videos or audio. Includes sites that provide information, tools or services related to text-to-speech, video, music, sound or image editing applications using AI with ability to generate new content.
- Generative AI - Text & Code: Sites that provide machine-generated text with broad domain applications (including code and translation) using AI and generating new content. Includes sites that provide tools or services that make suggestions, edits, review or create summaries based on user prompts and interactions.
- Hacking: Sites that provide information about or promote illegal or questionable access to or use of computer or communication equipment, software or databases.
- Information Technology: Sites sponsored by or providing information about computers, software, the Internet and related business firms, including sites supporting the sale of hardware, software, peripherals and services.
- Other AI ML Applications: Sites that provide tools or services related to artificial intelligence and machine learning. Includes sites hosting applications with personal productivity or business purposes using AI but not typically capable of generating new content.
- Proxy Avoidance: Sites that provide information about how to bypass proxy server features or to gain access to URLs in any way that bypasses the proxy server.
- Search Engines and Portals: Sites that support searching the web, news groups or indices or directories thereof.
- Web Analytics: Sites that are associated with web traffic analysis.
- Web and Email Marketing: Sites that are associated with online marketing.
- Web and Email Spam: Sites whose links are sent in unsolicited commercial email, either as part of campaigns to promote products or services or to entice readers to click through to surveys or similar sites. Also includes sites that display comment spam.
- Web Collaboration: Sites that provide virtual workspace for purposes of collaboration and conferencing, which may include sites that enable authorized access to a computer or network from a remote location.
- Web Hosting: Sites of organizations that provide hosting services, or top-level domain pages of web communities.
- Website Translation: Sites that enable translation of website text.

Internet Communication

Parent category that contains categories related to internet-based communication and exchange.

- General Email: Sites that provide email services open to general use.
- Organizational Email: Log in sites for corporate or institutional email systems.
- Text and Media Messaging: Sites that enable the sending of messages and other content through SMS, EMS, MMS, or similar protocols.
- Web Chat: Sites that host web chat services or that support or provide information about chat through HTTP or IRC.

Miscellaneous

Parent category that contains categories identified by URL attributes, not classified elsewhere.

- Content Delivery Networks: Commercial hosts that deliver content to subscribing websites.
- Dynamic Content: URLs that are generated dynamically by a web server.
- File Download Servers: Web servers whose primary function is to deliver files for download.
- Network Errors: URLs with hosts that do not resolve to IP addresses.
- Private IP Addresses: IP addresses defined in RFC 1918, 'Address Allocation for Private Intranets.'
- Uncategorized: Sites not categorized in the Primary Database.
- Web Images: Sites that deliver image content.
- Web Infrastructure: Sites that are associated with website architecture.

News and Media

The parent category that contains categories related to news, magazines, and other media.

- Alternative Journals: Online equivalents to supermarket tabloids and other fringe publications.
- News and Media: Sites that offer current news and opinion, including those sponsored by newspapers, general-circulation magazines or other media.

Productivity

Parent category that contains categories considered to affect productivity in a corporate environment.

- Advertisements: Sites that provide advertising graphics or other ad content files.
- Application and Software Download: Sites that enable download of software, applications.
- Instant Messaging: Sites that enable instant messaging.
- Message Boards and Forums: Sites that host message boards, bulletin boards and other unaffiliated discussion forums.
- Online Brokerage and Trading: Sites that support active trading of securities and investment management.
- Pay-to-Surf: Sites that reward users for online activity such as viewing websites, advertisements or email.

Religion

Parent category that contains categories related to religion.

- Lesser-Known Religions: Sites that provide information about or promote lesser known religions and religious beliefs.
- Widely-Known Religions: Sites that provide information about or promote more widely known religions and religious beliefs, including but not limited to Buddhism, Christianity, Hinduism, Islam, Judaism, Mormonism, Shinto and Sikhism, as well as atheism.

Security

Security-related website categories that allow you to develop policies to deny access to sites associated with spyware, phishing, keylogging, and malicious mobile code.

- Advanced Malware Command and Control: Protects against outbound transmissions from a compromised machine to a malicious command-and-control centre.
- Advanced Malware Payloads: Inbound network transmissions of payloads intended to exploit a machine.
- Bot Networks: Protects against outbound transmissions from a compromised machine to a malware command-and-control centre.
- Compromised Websites: Sites that are vulnerable and known to host an injected malicious code or unwanted content.
- Custom-Encrypted Uploads: Outbound network transmissions of documents, payloads, and data that have been encrypted using custom encryption methods.
- Files Containing Passwords: Documents and data that include lists of network passwords such as Unix and Windows user passwords; also, documents that potentially contain lists of usernames and passwords.
- Keyloggers: Sites that download programs that record all keystrokes, and which may send those keystrokes (potentially including passwords or confidential information) to an external party.
- Malicious Embedded Link: Sites infected with a malicious link.
- Malicious Embedded iFrame: Sites infected with a malicious iFrame.
- Malicious Websites: Sites containing code that may intentionally modify users' systems without their consent and cause harm.
- Mobile Malware: Protects against malicious websites and applications designed to run on mobile devices.
- Phishing and Other Frauds: Sites that counterfeit legitimate sites to elicit financial or other private information from users.
- Potentially Exploited Documents: Documents containing content with suspicious characteristics that could lead to the exploitation of a machine.
- Potentially Unwanted Software: Sites using technologies that alter the operation of a user's hardware, software or network in ways that diminish control over the user experience, privacy or the collection and distribution of personal information.
- Spyware: Sites that download software that generate HTTP traffic (other than simple user identification and validation) without a user's knowledge.
- Suspicious Embedded Link: Sites suspected of being infected with a malicious link.

Shopping

Parent category that contains categories related to shopping.

- Internet Auctions: Sites that support the offering and purchasing of goods between individuals.
- Real Estate: Sites that provide information about renting, buying, selling or financing residential real estate.
- Shopping: Sites that support the online purchase of consumer goods and services except: sexual materials, lingerie, swimwear, investments, medications, educational materials, computer software or hardware, alcohol, tobacco, travel, vehicles and parts, weapons.

Social Organizations

Parent category that contains categories of chartered groups or clubs, or similar social organizations.

- Professional and Worker Organizations: Sites sponsored by or that support or offer information about organizations devoted to professional advancement or workers' interests.
- Service and Philanthropic Organizations: Sites sponsored by or that support or offer information about organizations devoted to doing good as their primary activity.
- Social and Affiliation Organizations: Sites sponsored by or that support or offer information about organizations devoted chiefly to socializing or common interests other than philanthropy or professional advancement.

Social Web - Facebook

Category used to manage the Facebook domain. Contains:

- Facebook Apps : Facebook function that enables a user to access or utilize an app.
- Facebook Chat: Facebook function that enables a user to chat within the Facebook community.
- Facebook Commenting: Facebook function that enables a user to comment or like.
- Facebook Events: Facebook function that enables a user to create, modify or respond to an event within the Facebook community.
- Facebook Friends: Facebook function that enables a user to add a connection.
- Facebook Games: Facebook function that enables a user to access or play a game.
- Facebook Groups: Facebook function that enables a user to create, modify or join a group within the Facebook community.
- Facebook Mail: Facebook function that enables a user to send an email within the Facebook community.
- Facebook Photo Upload: Facebook function that enables a user to upload a photo.
- Facebook Posting: Facebook function that enables a user to share a post, status or link.
- Facebook Questions: Facebook function that enables a user to ask a question within the Facebook community.
- Facebook Video Upload: Facebook function that enables a user to upload a video.

Social Web - LinkedIn

Category used to manage the LinkedIn domain. Contains:

- LinkedIn Updates: LinkedIn function that enables a user to edit a profile or post an update.
- LinkedIn Mail: LinkedIn function that enables a user to send an email within the LinkedIn community.
- LinkedIn Connections: LinkedIn function that enables a user to add a connection.
- LinkedIn Jobs: LinkedIn function that enables a user to perform activities related to job search.

Social Web - Twitter

Category used to manage the Twitter domain. Contains:

- Twitter Posting: Twitter function that enables a user to post an update.
- Twitter Mail: Twitter function that enables a user to send an email within the Twitter community.
- Twitter Follow: Twitter function that enables a user to add a connection.

Social Web Controls - Various

Category used to manage various domain controls. Contains:

- Blog Commenting: General function that enables a user to post a comment.
- Blog Posting: General function that enables a user to post a blog entry.
- Classified Posting: General Function that enables a user to post a classified ad.

Social Web - YouTube

Category used to manage the YouTube domain. Contains:

- YouTube Commenting: YouTube function that enables a user to comment, like or dislike.
- YouTube Video Upload: YouTube function that enables a user to upload a video.
- YouTube Sharing: YouTube function that enables a user to share a video within and outside of the YouTube community.

Sports

Parent category that contains categories related to sports.

- Sport Hunting and Gun Clubs: Sites that provide information about or directories of gun clubs and similar groups, including war-game and paintball facilities.
- Sports: Sites that provide information about or promote sports, active games and recreation.

Stand-Alone Categories

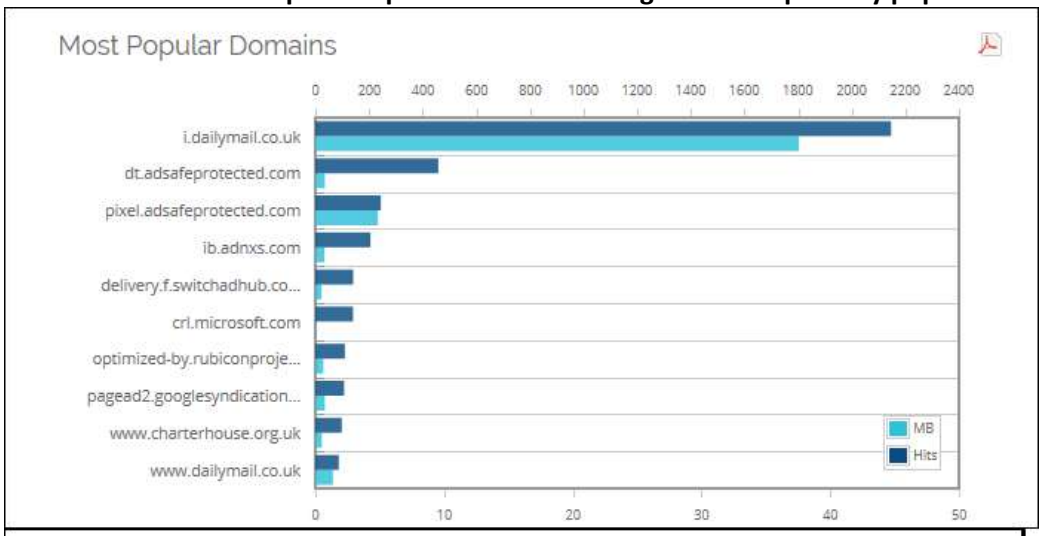
- Advocacy Groups: Sites that promote change or reform in public policy, public opinion, social practice, economic activities and relationships.
- Gambling: Sites that provide information about or promote gambling or support online gambling, involving a monetary exchange.
- Games: Sites that enable a user to play or download a game.
- Health: Sites that provide information or advice on personal health or medical services, procedures, devices, or self-help resources.
- Illegal or Unethical: Sites that promote or provide instruction in nonviolent crime or unethical behavior or the avoidance of prosecution.
- Internet Watch Foundation: Sites that offer content that, in the judgment of the Internet Watch Foundation (IWF), violates UK laws respecting child abuse (i.e., child pornography).
- Intolerance: Sites that condone intolerance towards any individual or group.
- Job Search: Sites that offer information about or support the seeking of employment or employees.
- Militancy and Extremist: Sites that offer information about or promote or are sponsored by groups advocating antigovernment beliefs or action.
- Parked Domain: Sites that are expired, offered for sale, or known to display targeted links and advertisements.
- Special Events: Sites devoted to a current event that requires separate categorization.
- Tasteless: Sites with content that is improper or unsuitable, but not violent.
- Travel: Sites that provide information about or promote travel-related services and destinations.
- Vehicles: Sites that provide information about or promote vehicles, including those that support online purchase of vehicles or parts.
- Violence: Sites that feature or promote violence or bodily harm, including self-inflicted harm; or that gratuitously display images of death, gore or injury; or that feature images or descriptions that are grotesque or frightening.

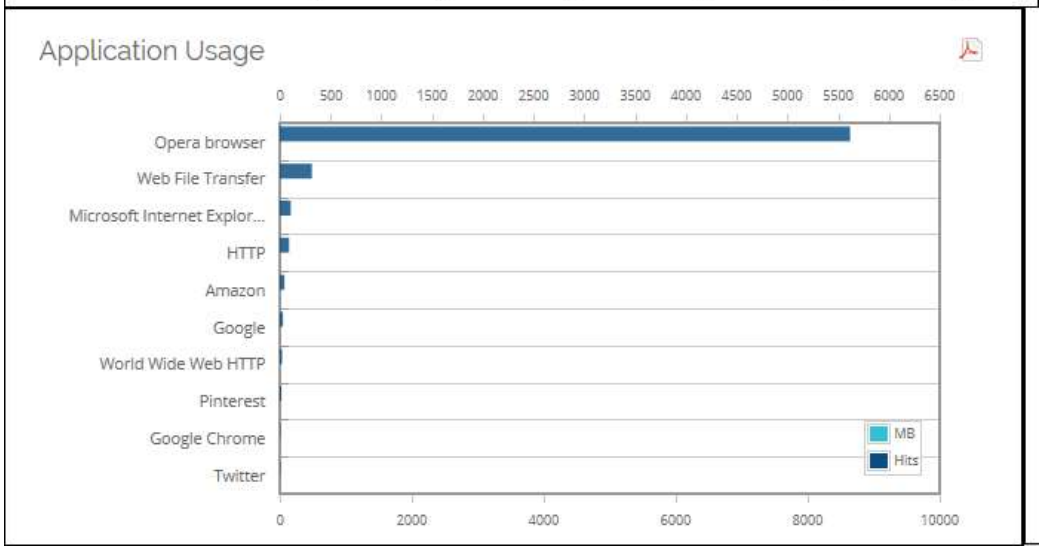
- Weapons: Sites that provide information about, promote, or support the sale of weapons and related items.

APPENDIX B: DATA KEPT ON PUPIL INTERNET USAGE FOR EACH ACCESS REQUEST ON THE FIREWALL SERVER

Date and time, pupil internet name, source IP address, destination IP address, port ID, internet line used, firewall policy and protocol, filtering category, application name, web destination, whether access was allowed or denied, total bytes used and total hits on that site by that user.

This data can then compiled to produce the following sorts of reports by pupil:





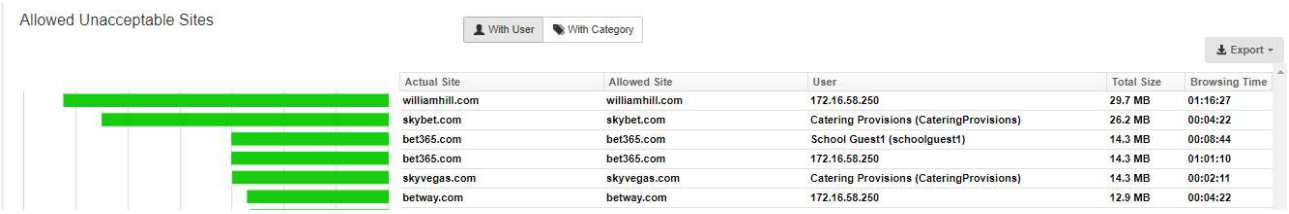
This data will be kept on the Firewall for up to 1 month.

APPENDIX C – EXAMPLE OF A COMPILED REPORT HELD ON THE DEPT.SHARES FOLDER AND IN THE ONLINE SAFETY TEAM

Date	Time from	Time to	Category	User	Visited site	Categorised site	Hits
23/01/2025	19:19:56	19:25:48	Weapons	(DAWNAC01)	google.com	warrelics.eu	2
23/01/2025	19:19:59	19:19:59	Weapons	(DAWNAC01)	google.com	history-making.com	1
23/01/2025	19:25:22	19:25:22	Weapons	(DAWNAC01)	google.com	worldwarcollectibles.com	1
23/01/2025	19:27:41	19:28:16	Weapons	(DAWNAC01)	google.com	heartsanddaggers.co.uk	2
23/01/2025	19:29:51	19:29:51	Weapons	(DAWNAC01)	google.com	centurionauctions.com	1
23/01/2025	17:28:08	17:28:08	Gambling	(CHAUAC01)	iivt.com	iivt.com	1
23/01/2025	17:28:08	17:28:13	Gambling	(CHAUAC01)	ladbrokes.com	ladbrokes.com	77
23/01/2025	18:50:30	18:50:31	Gambling	(CHAUAC01)	ladbrokes.com	ladbrokes.com	2
23/01/2025	15:05:26	15:05:37	Gambling	(THABAT01)	useamp.com	useamp.com	12

This report will be kept on the Department Shared folder and Online Safety Team for 24 months.

New reporting system being produced alongside the above report.



Actual Site	Allowed Site	User	Total Size	Browsing Time
williamhill.com	williamhill.com	172.16.58.250	29.7 MB	01:16:27
skybet.com	skybet.com	Catering Provisions (CateringProvisions)	26.2 MB	00:04:22
bet365.com	bet365.com	School Guest1 (schoolguest1)	14.3 MB	00:08:44
bet365.com	bet365.com	172.16.58.250	14.3 MB	01:01:10
skyvegas.com	skyvegas.com	Catering Provisions (CateringProvisions)	14.3 MB	00:02:11
betway.com	betway.com	172.16.58.250	12.9 MB	00:04:22

This report will be kept on the Department Shared folder and Online Safety team for 24 months.