



**CHARTERHOUSE**

## **IT E-Safety and Technical Security Policy**

## **DEFINITION OF THIS POLICY**

Effective technical security depends not only on technical measures but also on appropriate policies and procedures and on good user education and training. This policy outlines the steps that the School has taken in order to ensure the safety of pupils, staff and the School's network and infrastructure. The School will be responsible for ensuring 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 to monitoring purposes within the School's policies.
- Access to personal data is securely controlled
- There is effective guidance and training for staff
- There are regular reviews and audits of the safety and security of the School's computer systems

## **RESPONSIBILITIES**

The management of technical security will be the responsibility of the Head of IT Services.

## **TECHNICAL SECURITY**

The School will be responsible for ensuring that their infrastructure/network is as safe 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 technical requirements.
- there will be regular reviews and audits of the safety and security of the School's 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 from accidental or malicious attempts which might threaten the security of the School's 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 rights to the School's technical systems.
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their login details and must immediately report any suspicion or evidence that there has been a breach of security.
- Charterhouse technical staff regularly monitor and record the activity of users on the School technical systems and users are made aware of the in the acceptable use policy.

## **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 platforms.

- The School networks and systems are protected by secure passwords and 2FA where possible.
- 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 Network Manager and will be reviewed annually, by the online safety group.
- All users have the responsibility for the security of their username and password and must not allow others to access systems using their details.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by the IT Department.

## PASSWORD REQUIREMENTS

- Passwords should be long and complex, using three random words and numbers.
- 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 not include names or any other personal information about the user that might be known by others.
- Passwords must be changed on first login to the system.

## APPROPRIATE FILTERING FEATURES

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 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 the school.

The firewall / web filtering is provided by WatchGuard Technologies Inc., who hold the Friendly Wi-Fi certification, which is associated with the IWF (Internet Watch Foundation). The web-filtering element has a feed, which incorporates 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'.

Certain categories of websites are blocked at all times (see Appendix A for restricted categories) with additional restrictions such as social networking, 'Freeware', software downloads and online games during hashes and banco.

**Age appropriate** – All pupils (age range 13 -18) have the same internet filtering restrictions, although the evening cut off times vary from year group to year group as set out below:

10pm – 4ths

10.15pm – Removes

10.30pm – 5ths

11.30pm – Specialists

**Responsibility / Control** – The firewall / web filter is controlled and administered by the IT Department, who have the ability to add or remove certain websites from the filtering controls. To ensure there is a system of checks and balances and to protect those responsible, changes to the School filtering service must be agreed with the Online Safety Group.

All users have the responsibility to report immediately to the IT Department any infringements of the School filtering policy of which they become aware of 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.

**Circumvention** – The firewall allows the school to block known VPN's, Proxy services and DNS over HTTPS, although this is limited in its use without using deep packet inspection which brings its only limitations.

**Control** – The IT Department have the ability to control the levels of filtering.

**Filtering Policy** – WatchGuard use ‘Forcepoint’ web filtering and Appendix A gives a full overview of the website categorizations. Those highlighted in yellow are the categories currently blocked.

**Identification** – The web filter reporting allows the IT dept. to identify specific users and their devices, see Appendix C.

**Mobile and App Content** – Whenever a pupil uses a mobile device to connect to the internet via the School network the same level of filtering will be applied as with a laptop or PC.

**Multiple Language Support** – The firewall and web filter supports multiple languages.

**Network Level** – The firewall and web filtering is applied at network level and any device, which connects to the network, will go through the filtering process without having to add any additional software on their device.

**Reporting Mechanism** – The web filter retains information on accessed websites and attempts to access blocked websites on an individual level for up to 12 months, see Appendix B. This data is compiled and reported to the Assistant Head (Wellbeing), the Assistant Head (Pastoral) and the Designated Safeguarding Leads on a weekly basis via the CPOMS system, as well as on an ad hoc basis when needed. This compiled information is kept for up to 24 months.

**Reports** – See Appendix C.

## **APPROPRIATE MONITORING FEATURES**

**Age Appropriate** – Reports showing attempts to access certain categories of blocked websites (see Reporting below) are generated on a weekly basis and separated into Under School and Specialist pupils and sent to SLT and the DSL. Consideration can then be given to possible responses.

**BYOD** – Pupils are aware that all devices connected to the School network are subject to web filtering and reporting. This is part of the IT Pupil Acceptable Use policy and this is discussed with all new pupils as part of their IT induction at Charterhouse.

**Data Retention** – Data relating to pupils can be seen in Appendix B and is kept for up to 12 months.

**Flexibility** – Any changes in web filtering can be quickly added or removed by the IT dept. New websites are blocked until they have been assessed and categorised by the firewall provider.

**Impact** – This policy and working procedures are reviewed on a regular basis (at least Quarterly) by the Head of IT Services in order to ensure that they are fit for purpose.

**Monitoring Policy** – Pupils are asked to sign a copy of the IT Pupil Acceptable Use policy and copy is available on the School intranet. This is also discussed as part of the new pupil IT induction.

**Multiple Language Support** – The firewall and web filter supports multiple languages.

**Prioritisation** – The Head of IT Services produces and reviews the internet logs on a weekly basis and sends copies to the Assistant Head (Wellbeing), the Assistant Head (Pastoral) and the Designated Safeguarding Leads via the CPOMS system. Any immediate concerns are raised by the Head of IT Services.

**Reporting** – The categories that are reported are Abortion, Abused Drugs, Marijuana, Gambling, Illegal or Questionable, Intolerance, Militancy and Extremism, Alcohol and Tobacco, Sport Hunting and Gun Clubs, Violence and Weapons. Anorexia websites are categorised as violence but Charterhouse also blocks and reports on blog websites such as Pro Anorexia and Pro Suicide.

Concerns are recorded, in the first instance, by the Head of IT Services in the CPOMS system and then detailed reports are sent to the SLT and the Designated Safeguarding Leads. These reports are kept for up to 24 months.

**Limitations** – The web filtering does not record searches for websites, only websites requested. The School does not have keystroke software installed on any School owned devices and any cellular devices use their own mobile data so are outside of our monitoring system.

### **CYBERSENSE EDUCATION/TRAINING/AWARENESS**

Charterhouse does not look to block access to the internet via 3G or 4G mobile devices but looks to educate through its Cybersense programme.

In addition to this filtering and monitoring policy, Charterhouse also seeks to educate pupils to be safe on the internet with a structured education program based on the three C's; **Contact, Conduct and Content**.

**All Fourths** receive Cybersense sessions during their Monday activity sessions in LQ. These sessions include cyber safety, internet addiction, sexting, cyber bullying. This programme continues through the School with specific year groups receiving targeted workshops.

**Removes:** Body image in the media, the law around social media, consequences of online bullying.

**Fifths:** cyber-sense controversy/discussion cards, pornography (all workshop style), online media law (lecture).

### **STAFF TRAINING**

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

## APPENDIX A: FIREWALL CATEGORIES

*Categories highlighted in yellow are blocked at all times in compliance with the UK Safer internet Centre list. Those highlighted in green are blocked only during hash and banco times.*

*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

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 suggestive but not lewd costume, with semi nudity permitted. Includes classic 'cheesecake,' calendar and pinup art and photography. Includes sites offering lingerie or swimwear for sale.
- Nudity: Sites that offer depictions of nude or seminude human forms, singly or in groups, not overtly sexual in intent or effect.
- 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 information about sex and sexuality, with no pornographic intent.

### Advocacy Groups

Sites that promote change or reform in public policy, public opinion, social practice, economic activities and relationships.

### Bandwidth

Sites that use a large amount of bandwidth.

- 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 via 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 via network cameras, webcams and other video recording devices.
- Viral Video: Sites that host videos with high or rapidly rising popularity.

### 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**

Office Category used to manage the Office domain, and includes these functions:

- Office - Apps: Office function that enables a user to collaborate via various applications.
- Office - Documents: Office function that enables a user to collaborate via document applications.
- Office - Drive: Office function that enables a user to collaborate via virtual storage.
- Office - Mail: Office function that enables a user to collaborate via email and messaging.

### **Drugs**

The parent category that contains the following categories:

- 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**

The parent category that contains the following categories:

- Cultural Institutions: Sites sponsored by museums, galleries, theaters (but not movie theaters), libraries and similar institutions; also, sites whose purpose is the display of artworks.
- 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**

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**

The parent category that contains the following categories:

- 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: Scans for newly registered websites on an ongoing basis. The default criteria for classification under the associated category Newly Registered Websites involves unknown (Uncategorized) websites registered within the last 41 days. Exception is given to websites known to pose a live security risk; such websites are assigned security classification regardless of the registration attribute. A website classified under the category Newly Registered Websites may acquire a granular content-based category at any time.

- Suspicious Content: Sites found to contain suspicious content.

### **Gambling**

Sites that provide information about or promote gambling or support online gambling, involving a risk of losing money.

### **Games**

Sites that enable a user to play or download a game.

### **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.

### **Health**

Sites that provide information or advice on personal health or medical services, procedures, or devices, but not drugs. Includes self-help groups.

### **Illegal or Questionable**

Sites that provide instruction in or promote nonviolent crime or unethical or dishonest behavior or the avoidance of prosecution.

### **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.

- Computer Security: Sites that provide information about or free downloadable tools for computer security.
- Hacking: Sites that provide information about or promote illegal or questionable access to or use of computer or communication equipment, software or databases.
- 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.
- Unauthorized Mobile Marketplaces: Protects against websites that may distribute applications unauthorized by the mobile OS manufacturer, the handheld device manufacturer or the network provider. (Traffic visiting websites in this category may indicate jail-broken or rooted phones.)
- 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**

The parent category that contains the following categories:

- 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 via SMS, EMS, MMS or similar protocols.
- Web Chat: Sites that host web chat services or that support or provide information about chat via HTTP or IRC.

### **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 anti-government beliefs or action.

### **Miscellaneous**

The parent category that contains the following categories:

- 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.'
- Web Images: Sites that deliver image content.
- Web Infrastructure: Sites that are associated with website architecture.
- 

### **News and Media**

Sites that offer current news and opinion, including those sponsored by newspapers, general-circulation magazines or other media.

- Alternative Journals: Online equivalents to supermarket tabloids and other fringe publications.

### **Parked Domain**

Sites that are expired, offered for sale, or known to display targeted links and advertisements.

### **Productivity**

The parent category that contains the following categories:

- 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**

The parent category that contains the categories:

- Non-Traditional Religion: Sites that provide information about non-traditional religious beliefs and practices.
- Traditional Religions: Sites that provide information about or promote Bahai, Buddhism, Christian Science, 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 center.
- Bot Networks: Sites that host the command-and-control centers for networks of bots that have been installed onto users' computers. (Excludes web crawlers.)
- Compromised Websites: Sites that are vulnerable and known to host an injected malicious code or unwanted content.
- 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 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

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.

- 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.

## Social Organizations

The parent category that contains the following categories:

- 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.

### Social Web - LinkedIn

Category used to manage the LinkedIn domain.

### Social Web - Twitter

Category used to manage the Twitter domain.

### Social Web - YouTube

Category used to manage the YouTube domain.

## **Society and Lifestyles**

Sites that provide information about matters of daily life, excluding entertainment, health, hobbies, jobs, sex and sports.

- 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.
- Gay or Lesbian or Bisexual Interest: Sites that provide information about or cater to gay, lesbian, or bisexual lifestyles, but excluding those that are sexually or issue oriented.
- Hobbies: Sites that provide information about or promote private and largely sedentary pastimes, but not electronic, video or online games.
- 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.

## **Special Events**

Sites devoted to a current event that requires separate categorization.

## **Sports**

Sites that provide information about or promote sports, active games, and recreation.

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

## **Tasteless**

Sites with content that is gratuitously offensive or shocking, but not violent or frightening. Includes sites devoted in part or whole to scatology and similar topics or to improper language, humor or behavior.

## **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 and of no redeeming value.

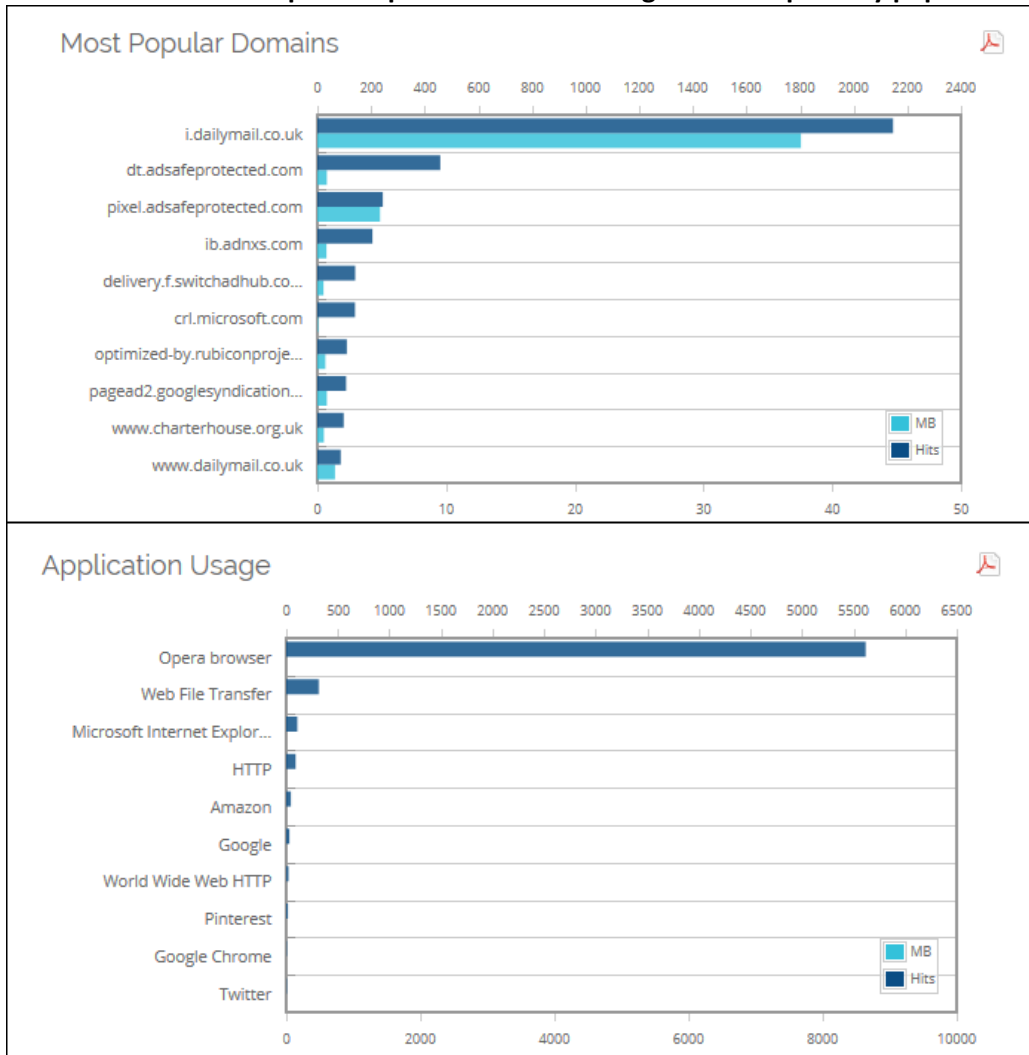
## **Weapons**

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 be compiled to produce the following sorts of reports by pupil:



This data will be kept on the Firewall for up to 12 months, depending on the volume of data hitting the firewall in any one period.

## APPENDIX C – EXAMPLE OF A COMPILED REPORT HELD ON THE DEPT.SHARES FOLDER

### Blocked website report

26/06/2021 19:39	GYTFREGEM01	Alcohol and Tobacco	<a href="http://www.thedrinksbusiness.com">www.thedrinksbusiness.com</a>
26/06/2021 10:03	GYTFREGEM02	Illegal or Questionable	<a href="http://b-ok.cc">b-ok.cc</a>
21/06/2021 08:22	HUNSGHHJ07	Prescribed Medications	<a href="http://www.medicspot.co.uk">www.medicspot.co.uk</a>
21/06/2021 18:34	HUNSGHHJ08	Alcohol and Tobacco	<a href="http://tools.group.adventurebar.co.uk">tools.group.adventurebar.co.uk</a>
21/06/2021 12:39	HUNSGHHJ09	Weapons	<a href="http://www.holtsauctioneers.com">www.holtsauctioneers.com</a>
22/06/2021 17:44	JECCGFTHS01	Alcohol and Tobacco	<a href="http://www.simplycigars.co.uk">www.simplycigars.co.uk</a>
21/06/2021 17:23	KUPOOYTH01	Prescribed Medications	<a href="http://www.medicspot.co.uk">www.medicspot.co.uk</a>
25/06/2021 14:20	KUPOOYTH01	Alcohol and Tobacco	<a href="http://www.porterhouse.london">www.porterhouse.london</a>
21/06/2021 14:40	KUPOOYTH01	Marijuana	<a href="http://www.leafly.com">www.leafly.com</a>
21/06/2021 17:51	NEWBLOUJ01	Alcohol and Tobacco	<a href="http://www.whatpub.com">www.whatpub.com</a>
25/06/2021 17:35	NEWBLOUJ01	Alcohol and Tobacco	<a href="http://www.luminour.it">www.luminour.it</a>

**This report will be kept on the Department Shared folder for 24 months.**