



St. Malachy's College

ESafety and DT Policy *October 2023*

ESafety and DT Policy

1 Introduction and Rationale

St Malachy's College promotes an environment in which students, staff and parents are committed to the idea of excellence within a caring, supportive community. The eSafety and Digital Technology Policy seeks to uphold the ethos of St Malachy's College as encapsulated in its Mission Statement and Motto:

'St Malachy's College, as a Catholic School, is dedicated to provide academic excellence in the context of a Christian community ethos. It seeks to preserve its traditions of spirituality and learning, so that all pupils and staff can experience continuity in achievement and further their own spiritual, educational and personal growth in a pleasant, interesting and stimulating environment'

The College Motto "Gloria Ab Intus", Glory from Within, illustrates that the fundamental ethos within the College is that of formative and holistic education "Gloria Ab Intus", reminds us all of the importance of 'Glory from within' and St Malachy's, as a Catholic school seeks to recognise and respect the uniqueness of all individuals, to enable them to reach their full potential and to help create the world as God intends it to be.

The College is committed to the use of digital technology and to this end we have recently attracted investment to complete the building of a creative digital technology hub, providing learners with new and exciting learning experiences and opportunities.

It is the responsibility of the College to mitigate risk through reasonable planning and actions. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. eSafety covers not only Internet technologies but also a range of other electronic communications including mobile phones, games consoles and wireless technology.

The College must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The eSafety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young

people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use. This policy operates in conjunction with other relevant policies and procedures including Positive Behaviour, Anti-Bullying, Child Protection and Remote Learning.

In the majority of areas within the school, the College uses the Education Authority funded C2k Education Network. However, having given regard to DENI Circular Number: 2016/27 the Creative Digital Hub operates on a separate network, and it uses a web filtering system provided by a secure Draytek Vigor Router (Appendix 1).

2. Aims

1. To promote the safe and effective use of digital technology by students and staff to improve learning and teaching and enhance career opportunities.
2. To ensure that students are confident with emerging digital technologies and understand the benefits but also the risks.
3. To support students to safeguard themselves while using digital technology both inside and outside of school.
4. To raise student awareness of unsafe situations online and what to do if they feel unsafe.
5. To educate students on digital technology risks, misuse and the possible legal implications of misuse.
6. To ensure that students and staff are appropriately protected through the College c2k network and the Digital Hub network.
7. To monitor eSafety incidents to inform future eSafety education and development.
8. To keep parents/ carers informed of any eSafety developments and help them support and guide their son.

ESafety and DT Policy

3. Definition of ESafety and Digital Technology

The DE eSafety Strategy Consultation Document (March 2019) states that:

“**eSafety** is about using electronic devices in a safe, responsible and respectful way. It means safeguarding children and young people in the digital world and educating them to keep themselves safe online.”

Furthermore, DE Keeping Children Safe in Education (September 2021) states that eSafety can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content; for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example: making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Digital Technology covers the electronic equipment, networking facilities, online services, digital media and software applications used to create, store, process, analyse and present digital information.

4. Scope of the Policy

This policy applies to **all** members of the College community who have access to and are users of the College's ICT network, both in and out of school. If incidents occur during school hours which contravene this Policy we will work with parents, staff and students to ensure eSafety of all involved, apply sanctions as appropriate and review procedures. If necessary, eSafety incidents will be reported to the PSNI or other relevant external agencies. **eSafety incidents which occur outside school hours are primarily the responsibility of parents.** If inappropriate activity occurs outside school hours with the intention of having a negative effect on any member of the College community, and this is brought to our attention, then we may liaise with parents as to an appropriate way forward.

5. Roles and Responsibilities

The Board of Governors

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy. Governors may avail of any relevant training.

The designated eSafety Governor is Mr. F MacElhatton. He will:

- Meet with the eSafety Officers as required
- Be informed of any eSafety incidents

Principal

The Principal is responsible for ensuring the safety (including eSafety) of members of the school community though day-to-day responsibility for eSafety will be delegated to the eSafety Officers. The Principal will be kept informed about eSafety incidents.

The Principal will deal with any serious eSafety allegation being made against a member of staff.

ESafety and DT Policy

ESafety Committee

The eSafety Committee is comprised of the members listed below:

| | |
|----------------|--|
| Mrs L Graham | VP Curriculum, C2 Manager and ESafety Officer |
| Mrs D McCusker | VP Pastoral, Designated Teacher for CP and ESafety Officer |
| Mr R Crozier | HOD ICT |
| Mrs C McGrath | Creative Digital Hub Leader |
| Mr S Millar | IT Manager & C2 Manager |
| Mr T Crooks | Creative Technologist |

e-Safety Officers

The role is shared between the two Vice Principals; the Curriculum VP is also a C2K Manager and the Pastoral VP is the Designated Teacher for Child Protection.

The e-Safety Officers will:

- Take day to day responsibility for eSafety issues and have a leading role in establishing and reviewing the College eSafety policies / documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
- Liaise with C2K, Capita, and College ICT support staff as required
- Receive reports of eSafety incidents and create a log of incidents to inform future eSafety developments

The eSafety Committee will assist with:

- the review of the College's eSafety Policy and related documents and circulars;
- mapping and reviewing the eSafety curricular provision in the College;
- liaising with the ICT Manager regarding any reported incidents;
- liaising with pastoral staff and the Safeguarding Team

as required regarding any Safeguarding and Child Protection issues arising from incidents;

- consulting students and parents about eSafety provision.

The IT Manager will:

- Play a lead role in reviewing and updating the College's eSafety policy.
- Take a lead role as one of the C2K Managers, alongside the VP Curriculum, ensuring good communication between C2k, Capita and the College
- Ensure the College C2K users may only access the networks through properly enforced password protection;
- Reports any found issues with the filtering policies to C2K;
- Ensure that they keep up-to-date with eSafety good practice in order to effectively advise in their eSafety role;
- Ensure that they report any suspected misuse or a breach in eSafety to the eSafety Officers.
- Ensure where appropriate, they report any breach in eSafety to C2k;
- Ensure the "administrator" passwords for the College IT systems, used by the IT Manager, are also available to the Principal and kept in a secure place.
- Ensure usernames are only available for current staff and students. Additional users, e.g. exam users, guest users and substitute teachers are checked on a regular basis.
- Ensure any user under investigation for inappropriate use of the system is disabled promptly.
- Develop and facilitate induction and training seminars for staff and students when required.
- Assist with any investigation into reported cases of unacceptable content on social networking sites associated with the College community. Liaise with eSafety Officers and outside agencies on its removal and identification of personnel involved.

ESafety and DT Policy

Head of IT will:

- Assist in reviewing and updating the College's eSafety policy.
- Ensure that all students and staff within the IT department are aware of the procedures that need to be followed in the event of an eSafety incident taking place
- Liaise with the ICT Manager and C2k as required
- Be aware of relevant eSafety developments and communicate to staff as required

The Creative Digital Hub Leader will:

- Assist in reviewing and updating the College's eSafety policy.
- Oversee the work of the Creative Technologist.
- Assist in relevant aspects of the planning, design, specification and installation of the Digital Hub network systems.
- Along with the Creative Technologist liaise with managed service providers as required on changes to the Digital Hub infrastructure.
- Ensure that internet use across the system is monitored and that appropriate security levels for students and staff are set.
- Assist with any investigation into reported cases of viewing unacceptable content within the Hub network and identification of personnel involved
- Manage and monitor online activity in the Hub, taking appropriate action on discovery of offensive behaviour

The Creative Technologist will:

- Monitor and ensure safe internet usage, filtering system, and security level settings for students and staff.
- Assist with any investigation into reported cases of viewing unacceptable content and identification of personnel involved.
- Manage and monitor online activity, taking appropriate action on discovery of offensive behaviour.

- Help enable staff and students to reset passwords and log into the devices in the Digital Hub.
- Assist in reviewing and updating the College's eSafety policy.
- Comply with the requirements of the Data Protection Act and Copyright Laws, Computer Misuse action and Health and Safety at Work Act.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of eSafety matters and of the current school eSafety policy and practices.
- They adhere to the College's eSafety and Digital Technology Policy and that they have read, understood and signed the College Staff Acceptable Use Policy.
- They report any suspected misuse or problem to the eSafety Officers
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- They undertake all eSafety training as organised by the College

Students

Are responsible for ensuring that:

- They use the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to the College's systems. Appendix 3
- They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They know and understand College policies on the use of mobile phone, digital cameras and personal devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

(Continued overleaf)

ESafety and DT Policy

- They understand the importance of adopting good eSafety practice when using digital technologies out of school and realise that the College's eSafety Policy covers their actions out of school, if related to their membership of the school.

Parents

Parents are responsible for:

- their son's out-of-school online use of all C2k services and College devices;
- monitoring their son's appropriate use of digital technology outside of school hours;
- ensuring that their son complies with the age restrictions on Social Media Services.

6 Security Measures

The C2k Education Network ensures that a range of security measures is in place to secure the College and its users against potential risks. These include: firewalls; intrusion prevention systems; content filtering; email scanning and filtering; secure hosted applications; ongoing vulnerabilities assessment; user authentication using encryption and data security.

7 Email Security and Filtering of Internet Access

All staff and students are given access to the College's C2k email system. Individual usernames and passwords must be kept private. Staff must not use personal email accounts for school business or communicating with students. The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email, ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content. Staff and pupils accessing the Internet via the C2k Education Network will be required to authenticate using their C2k username and password. This authentication will provide Internet filtering via the C2k Education Network solution. Access to the Internet via the C2k Education Network is fully auditable and reports are available to the

school Principal. Connection of non C2k devices to the Internet e.g. iPads and other personal devices is through the controlled C2k wireless network and is subject to the same level of filtering as the main school system.

The Education Authority/C2k provides a filtered Internet service for schools in Northern Ireland. This is provided as part of the core C2kEn NI service in all schools. As a result, the following categories of websites are not, by default, available to users:

- **adult:** content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity;
- **violence:** content containing graphically violent images, video or text;
- **hate material:** content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds;
- **illegal drug taking and the promotion of illegal drug use:** content relating to the use or promotion of illegal drugs or misuse of prescription drugs;
- **criminal skill/activity:** content relating to the promotion of criminal and other activities;
- **gambling:** content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice.

As outlined in Section 1 of this policy, the Digital Hub does not run through the C2k network. Sites and software surrounding 'Gaming' and 'Esports' in particular are among those that are blocked by the C2k network, and this is software that is used by the Creative Digital Hub. These sites and software also require a large amount of bandwidth when running at full capacity and this is not something the C2k network in St. Malachy's College can handle. The Creative Digital Hub uses a Draytek Vigor Filtering System.

There are 3 different types of filter provided by this system which are explained in more detail in Appendix 1.

1. (GlobalView) Web-Content Filtering (WCF)
2. URL-Content Filtering
3. DNS Filtering

A filtering service, no matter how thorough, can never be guaranteed. If, at any time, students or school staff find themselves able to access inappropriate material which they think should be blocked, they should inform a member of staff/the IT Manager.

8 *ESafety Education*

The College actively promotes eSafety through the Preventative Curriculum. This takes place across a number of areas:

- Lessons within the Digital Hub and wider ICT and Computing Curriculum
- Safe use of Google Classroom
- Promotion of the Safer Schools App
- Form Tutorial and Assemblies including the involvement of external agencies
- Focus on the legal implications of inappropriate use of digital technology

Students will be helped to understand the need for the student Acceptable Use of Digital Technology Policy and encouraged to adopt safe and responsible use of digital technology outside of school.

eSafety Education is strongly linked to the Anti-Bullying Policy and education around Cyber Bullying is also a focus of the preventative curriculum. More information on this is located within the College Anti-Bullying Policy.

Creative Digital Hub Network Security

Introduction

Schools in Northern Ireland, including St Malachy's College, make use of the C2K network for IT services and security. It is a very safe network to use, but it comes with its limitations, which include guaranteed bandwidth and access to certain sites and software even though they are for educational purposes.

Sites and software surrounding 'Gaming' and 'Esports' in particular are among those that are blocked by the C2K network, and this is software that is used by the Creative Digital Hub. These sites and software also require a large amount of bandwidth when running at full capacity and this is not something the C2K network in St Malachy's College can handle, therefore we are managing our own.

The Creative Digital Hub uses a Draytek Vigor Filtering System.

There are 3 different types of filter provided by this system which will be explained in more detail.

1. (GlobalView) Web-Content Filtering (WCF)
2. URL-Content Filtering

3. DNS Filtering

The WCF in type 1 is also helped with the 'Google Safe Search' setting enabled on the browser.

Another layer of security is also added on top of the Filtering System by the Creative Digital Hub Server (server-to-server and client-to-server). With the use of the server, files or applications of any type can be blocked so that they are inaccessible to the end-user unless they are authorised.

1. GlobalView Web-Content Filtering

DrayTek's GlobalView Web-Content Filter is used to block any internet user from accessing inappropriate websites. Its database holds records of millions of websites, each one categorised according to their content type as shown below. The database is continuously updated, with new sites and also sites which spread malware.

These are the categories that the GlobalView WCF is blocking/filtering in the CDH network.

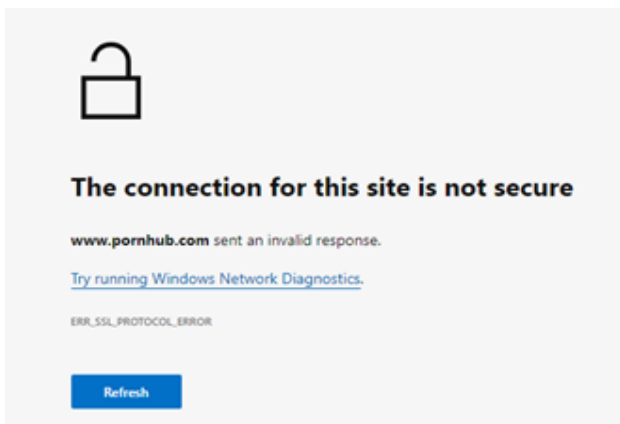
| | | | |
|---|--|---|---|
| <input type="button" value="Select All"/> | <input checked="" type="checkbox"/> Anonymizers | <input checked="" type="checkbox"/> Botnets | <input checked="" type="checkbox"/> Compromised |
| <input type="button" value="Clear All"/> | <input checked="" type="checkbox"/> Malware | <input type="checkbox"/> Network Errors | <input checked="" type="checkbox"/> Parked Domains |
| | <input checked="" type="checkbox"/> Phishing & Fraud | <input checked="" type="checkbox"/> Spam Sites | |
| | Advanced Categories | | |
| | <input type="checkbox"/> Cryptocurrency Mining | <input type="checkbox"/> Suspected Malware | <input type="checkbox"/> Suspected Phishing |
| Parental Control | Basic Categories | | |
| <input type="button" value="Select All"/> | <input checked="" type="checkbox"/> Alcohol & Tobacco | <input checked="" type="checkbox"/> Chat | <input checked="" type="checkbox"/> Child Abuse Images |
| <input type="button" value="Clear All"/> | <input checked="" type="checkbox"/> Criminal Activity | <input checked="" type="checkbox"/> Cults | <input checked="" type="checkbox"/> Hate & Intolerance |
| | <input checked="" type="checkbox"/> Illegal Drugs | <input checked="" type="checkbox"/> Nudity | <input checked="" type="checkbox"/> Pornography/Sexually Explicit |
| | <input checked="" type="checkbox"/> School Cheating | <input checked="" type="checkbox"/> Sex Education | <input checked="" type="checkbox"/> Tasteless |
| | <input checked="" type="checkbox"/> Violence | <input checked="" type="checkbox"/> Weapons | |
| | Advanced Categories | | |
| | <input type="checkbox"/> Child Inappropriate | <input type="checkbox"/> Gay or Lesbian or Bisexual | <input type="checkbox"/> Lingerie & Swimsuits |
| | <input type="checkbox"/> Marijuana | <input type="checkbox"/> Self-Harm | |
| Productivity | Basic Categories | | |
| <input type="button" value="Select All"/> | <input checked="" type="checkbox"/> Advertisements & Pop-Ups | <input type="checkbox"/> Computers & Technology | <input checked="" type="checkbox"/> Dating & Personals |
| <input type="button" value="Clear All"/> | <input type="checkbox"/> Download Sites | <input checked="" type="checkbox"/> Gambling | <input type="checkbox"/> Games |
| | <input checked="" type="checkbox"/> Hacking | <input checked="" type="checkbox"/> Illegal Software | <input type="checkbox"/> Image Sharing |
| | <input checked="" type="checkbox"/> Instant Messaging | <input type="checkbox"/> Job Search | <input type="checkbox"/> Peer-to-Peer |
| | <input type="checkbox"/> Shopping | <input checked="" type="checkbox"/> Social Networking | <input type="checkbox"/> Sports |
| | <input type="checkbox"/> Streaming Media & Downloads | | |
| | Advanced Categories | | |
| | <input type="checkbox"/> File Repository | <input type="checkbox"/> Remote Access | <input type="checkbox"/> Command and Control |
| General Use | Basic Categories | | |
| <input type="button" value="Select All"/> | <input type="checkbox"/> Arts | <input type="checkbox"/> Business | <input type="checkbox"/> Education |
| <input type="button" value="Clear All"/> | <input type="checkbox"/> Entertainment | <input type="checkbox"/> Fashion & Beauty | <input type="checkbox"/> Finance |
| | <input type="checkbox"/> Forums & Newsgroups | <input type="checkbox"/> General | <input type="checkbox"/> Government |
| | <input type="checkbox"/> Greeting Card | <input type="checkbox"/> Health & Medicine | <input type="checkbox"/> Information Security |
| | <input type="checkbox"/> Leisure & Recreation | <input type="checkbox"/> News | <input type="checkbox"/> Non-Profit & NGOs |
| | <input checked="" type="checkbox"/> Personal Sites | <input type="checkbox"/> Politics & Law | <input type="checkbox"/> Private IP Addresses |
| | <input checked="" type="checkbox"/> Real Estate | <input type="checkbox"/> Religion | <input type="checkbox"/> Restaurants, Food & Dining |
| | <input type="checkbox"/> Search Engines & Portals | <input type="checkbox"/> Translators | <input type="checkbox"/> Transportation |
| | <input type="checkbox"/> Travel | <input type="checkbox"/> Web-Based Email | <input checked="" type="checkbox"/> Uncategorized Sites |

Creative Digital Hub Network Security

When a user tries to access any of the sites that fall under any of these categories, it will be automatically blocked (and will therefore be inaccessible) and the following message will be returned:

“The connection for this site is not secure
(Insert URL here) sent an invalid response.”

For example:



1.1 Google Safesearch

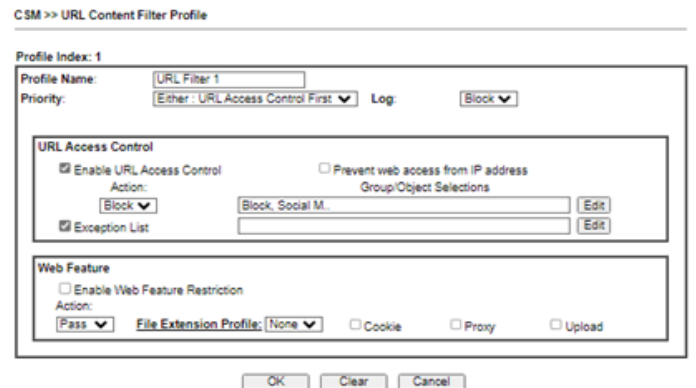
The Creative Digital Hub utilises ‘Google SafeSearch’ which is a setting that can be enabled on Google’s Chrome browser, the browser of choice in the Creative Digital Hub. This blocks content that Google deems inappropriate from search results (so that even the links of inappropriate material cannot be seen) and it is constantly updated and refreshed by Google.

Note: SafeSearch only works on Google search results, so it does not apply to other browsers such as Yahoo or Microsoft Bing. However, users cannot use these browsers anyway because our Filtering system will have blocked them.

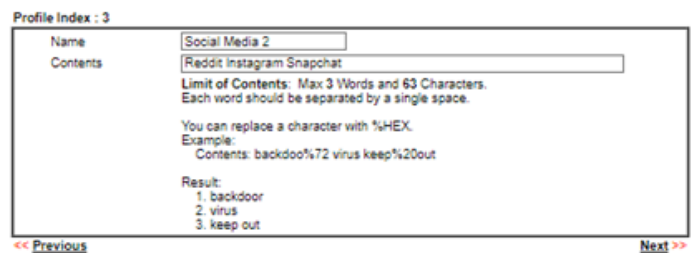
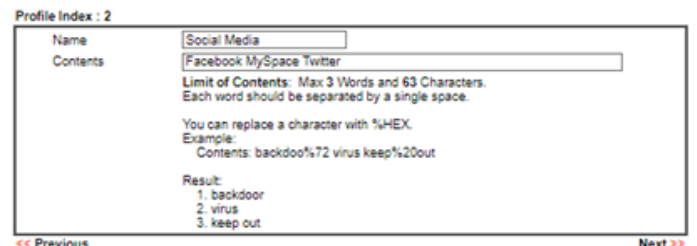
2. URL-Content Filtering

Draytek’s URL Filtering service allows for specific websites to be blocked/filtered (known as blacklisting) or unblocked (whitelisting). This would be used if a useful and safe website fell under a particular category that was blocked. We could whitelist it. Or if we deemed something to be inappropriate within an unblocked category, we could

blacklist it. This can be applied to search terms, keywords and IP addresses also.



Objects Setting >> Keyword Object Setup



3. DNS Filtering

Draytek’s DNS Filtering service blocks the domain names of websites. This means that instead of blocking the URL of a website, which can be circumvented (e.g. Google can still be accessed even if you block google.co.uk, by using google.co.jp (japan)), the entire domain for google can be blocked so that any request from the google DNS will be invalidated and rejected by the network and thus disallowing access.

Creative Digital Hub Network Security

DNS Filter Profile Table [Set to Factory Default](#)

| Profile | Name | Profile | Name |
|-----------|-------|-----------|------|
| <u>1.</u> | DNS 1 | <u>5.</u> | |
| <u>2.</u> | | <u>6.</u> | |
| <u>3.</u> | | <u>7.</u> | |
| <u>4.</u> | | <u>8.</u> | |

Note:
To make DNS Filter profile effective, please go to **Firewall >> Filter Setup** page to create a firewall rule and select the desired profile.

DNS Filter Local Setting

DNS Filter Enable

Web Content Filter WCF-1 St. Malachys DH

URL Content Filter UFC-1 URL Filter 1

Syslog None

Black/White List Enable Blacklist

Address Type Any Address

Start IP Address 0.0.0.0

End IP Address 0.0.0.0

Subnet Mask 0.0.0.0

IP Group None

or **IP Group** None

or **IP Object** None

or **IP Object** None

Administration Message (Max 255 characters) Default Message

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL% <br>that is categorized with %CL% <br>has been blocked by %RNAME% DNS Filter. <br><p>Please contact your system administrator for further information.</center></body>
```

Legend:
%SIP% - Source IP , %URL% - URL
%CL% - Category , %RNAME% - Router Name

Index No. 1

Profile Name DNS 1

Web Content Filter WCF-1 St. Malachys DH

URL Content Filter UFC-1 URL Filter 1

Syslog Block Only

Advanced Setting

Block DoT(DNS over TLS)

Block DoH(DNS over HTTPS)

Default DoH Servers

| Enable | Provider |
|-------------------------------------|---------------|
| <input checked="" type="checkbox"/> | Google |
| <input checked="" type="checkbox"/> | Cloudflare |
| <input checked="" type="checkbox"/> | OpenDNS |
| <input type="checkbox"/> | NextDNS |
| <input type="checkbox"/> | Quad9 |
| <input type="checkbox"/> | CleanBrowsing |

Customized DoH Server (Up to 8)

At least add one string object. [Objects Setting >> String Object](#)

Note:
DNS Filter does not work in DoH/DoT environment.
You can block DoH/DoT to force end-user to use standard DNS.

Google, CloudFlare & OpenDNS provide domain names that may potentially be malicious and can automatically block them. These data entries for the DNS names are automatically updated.

Creative Digital Hub Network Security

4 Server-to-Server & Client-to-Server

The Creative Digital Hub utilises a GPO (Group Policy) that secures network systems using a server.

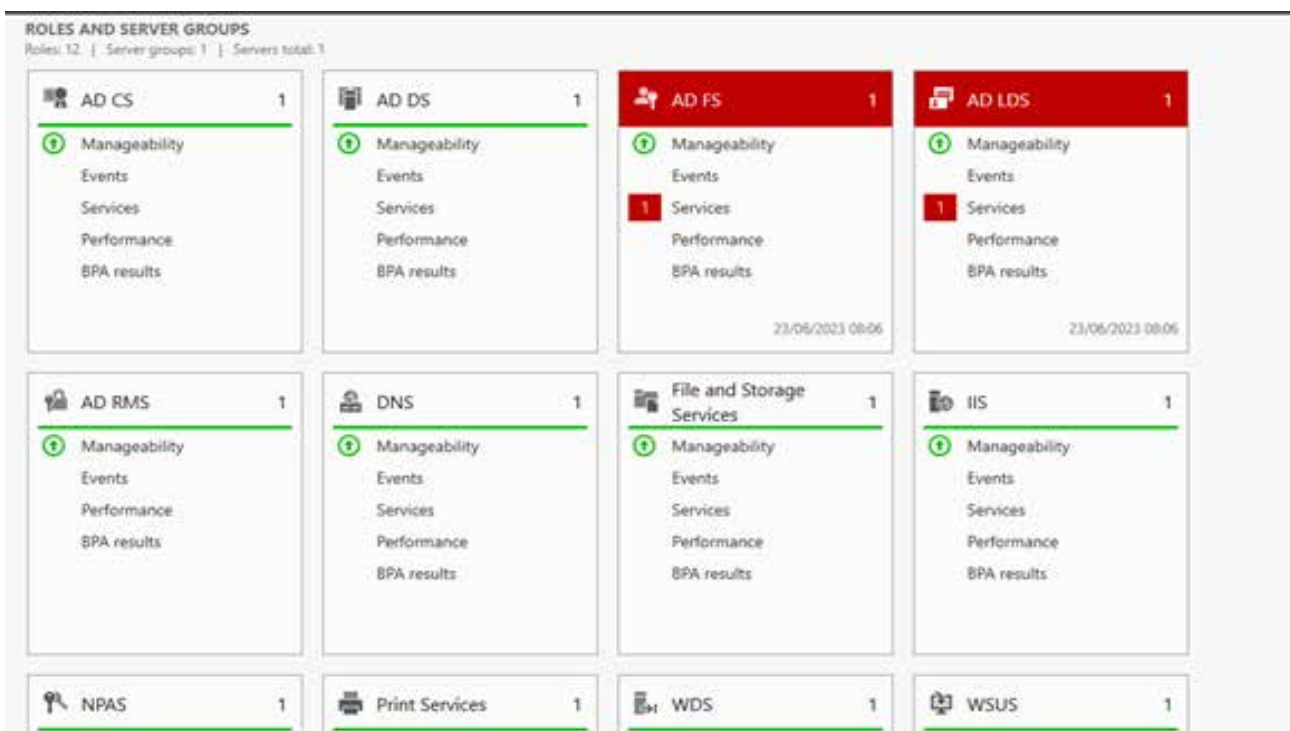
The server disallows students to stay signed in on any machine (which reduces the risk of personal accounts and data being used / stolen), to access or change settings on the machines or server.

Only the system administrator(s) have access to the server
































and to changes of settings on the machines.

Also any requests made to access a blocked DNS, URL or Search term, will be logged by the server, which will show the computer that was used and the exact time it was accessed at.

If any unauthorised access to any sites occur, it will be logged and investigated.



Creative Digital Hub *Network Security*

| | |
|---|-------------------------------|
|  Microsoft network server: Attempt S4U2Self to obtain claim ... | Not Defined |
|  Microsoft network server: Digitally sign communications (al... | Enabled |
|  Microsoft network server: Digitally sign communications (if ... | Enabled |
|  Microsoft network server: Disconnect clients when logon ho... | Enabled |
|  Microsoft network server: Server SPN target name validation... | Not Defined |
|  Network access: Allow anonymous SID/Name translation | Disabled |
|  Network access: Do not allow anonymous enumeration of S... | Enabled |
|  Network access: Do not allow anonymous enumeration of S... | Disabled |
|  Network access: Do not allow storage of passwords and cre... | Disabled |
|  Network access: Let Everyone permissions apply to anonym... | Disabled |
|  Network access: Named Pipes that can be accessed anonym... | ,netlogon,samr,lsarpc |
|  Network access: Remotely accessible registry paths | System\CurrentControlS... |
|  Network access: Remotely accessible registry paths and sub... | System\CurrentControlS... |
|  Network access: Restrict anonymous access to Named Pipes... | Enabled |
|  Network access: Restrict clients allowed to make remote call... | Not Defined |
|  Network access: Shares that can be accessed anonymously | Not Defined |
|  Network access: Sharing and security model for local accou... | Classic - local users auth... |
|  Network security: Allow Local System to use computer ident... | Not Defined |
|  Network security: Allow LocalSystem NULL session fallback | Not Defined |
|  Network security: Allow PKU2U authentication requests to t... | Not Defined |
|  Network security: Configure encryption types allowed for Ke... | Not Defined |
|  Network security: Do not store LAN Manager hash value on ... | Enabled |
|  Network security: Force logoff when logon hours expire | Disabled |
|  Network security: LAN Manager authentication level | Not Defined |
|  Network security: LDAP client signing requirements | Negotiate signing |
|  Network security: Minimum session security for NTLM SSP ... | Require 128-bit encrypti... |
|  Network security: Minimum session security for NTLM SSP ... | Require 128-bit encrypti... |
|  Network security: Restrict NTLM: Add remote server excepti... | Not Defined |
|  Network security: Restrict NTLM: Add server exceptions in t... | Not Defined |
|  Network security: Restrict NTLM: Audit Incoming NTLM Traf... | Not Defined |
|  Network security: Restrict NTLM: Audit NTLM authenticatio... | Not Defined |

Acceptable Use of Digital Technology *Staff*

In St Malachy's College staff are expected to abide by the Acceptable Use Policy for ESafety and Digital Technology.

1 Monitoring

The College has the right to access all C2k and Digital Hub user data, including cloud services and mailboxes. Files stored within the College's network environment on servers, computers and devices will not be regarded as private and the College reserves the right (or C2k at the College's request) to monitor, review and examine the Internet history, usage, communications and files of all users, and, where it deems it to be necessary, will intercept and delete material on school laptops, servers, network devices and email systems, which it considers inappropriate, and prohibit the use of such material.

There is automatic filtering of all C2k mail for unsuitable content and for size. Mail, which is blocked, may be viewed by the eSafety Officers (Vice Principals) who can then make a decision whether to allow the mail through the system and/or whether to take appropriate action within the terms of this eSafety and Digital Technology Policy.

2 General Responsibilities

- 2.1 Staff must conduct themselves responsibly and honestly when using Digital Technology. They must ensure that their actions do not:
 - 2.1.1 breach any law or statute, including data protection/GDPR guidelines; or otherwise bring the College into disrepute;
 - 2.1.2 waste time or resources;
 - 2.1.3 cause offence to colleagues or others.
- 2.2 Staff must not intentionally access, archive, store, distribute, edit, record, or reproduce any kind of inappropriate material on any of the College's Digital Technology devices or platforms or on their personal devices while on the College Site or when with students.
- 2.3 Staff must view in advance any digital content, especially online content, to be used with students to ensure it is appropriate. Advice should if necessary be sought from the relevant HOD or HOY and if required checked with the Designated Teacher.

- 2.4 All email communication with the wider school community must take place using c2k College accounts.
- 2.5 Staff should understand the importance of adopting good eSafety practice when using Digital Technology outside school and realise that the College's eSafety and Digital Technology Policy covers their actions outside school, if related to their membership of the school or involving any member of the school community.
- 2.6 Staff must ensure they adhere to The Copyright, Designs and Patents Act.
- 2.7 Staff monitor student use of all Digital Technology and implement current College policies with regard to their misuse:
 - 2.7.1 They report any suspected online misuse or a breach in eSafety to the Head of Year or the IT Manager as appropriate;
 - 2.7.2 They report child protection concerns to the Designated Teacher for Child Protection or Deputy Designated Teacher;
 - 2.7.3 They are aware of eSafety issues related to the use of Digital Technology and incorporate these into their teaching where relevant within pastoral and academic SOW.

3 Security

- 3.1 Staff must keep all passwords and user IDs confidential. The sharing of user IDs or passwords is prohibited at all levels. Users should ensure that strong passwords are used and stored securely.
- 3.2 Staff should log off or 'lock' a digital device, if leaving unattended, to prevent unauthorised use of their accounts.
- 3.3 It is the responsibility of users to ensure that confidential information (including photographs of students) is collected, stored and shared in compliance with General Data Protection Regulations.

Acceptable Use of Digital Technology *Staff*

4 *Software*

- 4.1 Staff must only acquire software with a direct educational use and have obtained permission from the ICT Manager (who can check c2k licencing issues).

5 *Mobile Devices*

- 5.1 Staff should adopt a professional approach when using personal mobile devices. Staff should only use mobile phones in front of pupils for school related business or emergency personal use.
- 5.2 Staff provided with mobile devices for official business while away from College official premises, must take the necessary security precautions to avoid damage or loss or misuse by a third party.
- 5.3 Staff must not leave College digital devices in a car or in a place where they would be visible to thieves. If College digital devices are used at home, they must be stored securely.

6 *Work Related Use of Social Networking*

All social networking for the College must operate via the official College networking sites. Posts should be forwarded to the Principal's PA. Posts involving photographs of pupils should not contain the full name of the pupil. Staff must check that any pupil pictured in a post has permission for his photograph to be used. If relevant staff must ensure that students are complying with Uniform Regulations in posts.

7 *Code of Conduct for All Staff and Volunteers* *(Child Protection/Safeguarding Policy)*

Staff should adhere to the College Code of Conduct with regards to any aspect of eSafety and Digital Technology. The Code of Conduct is Appendix 8 of the Child Protection Policy. It is incorporated into staff CP training and should be read in conjunction with this Acceptable Use Policy.

Agreement

All permanent and temporary staff who have been granted the right to use the College's Digital Technology are required to confirm by signature their understanding, acceptance and willingness to adhere to the College's eSafety and Digital Technology Policy.

Acceptable Use of Digital Technology *Students*

In St Malachy's College all students are expected to abide by the Acceptable Use Policy for ESafety and Digital Technology.

1 *Monitoring*

The College has the right to access all C2k and Digital Hub students' data, including cloud services and mailboxes. Files stored within the College's network environment on servers, computers and devices will not be regarded as private and the College reserves the right (or C2k at the College's request) to monitor, review and examine the Internet history, usage, communications and files of all users, and, where it deems it to be necessary, will intercept and delete material on digital devices and email systems, which it considers inappropriate, and prohibit the use of such material.

There is automatic filtering of all C2k mail for unsuitable content and for size. Mail, which is blocked, will be viewed by the eSafety Officers (Vice Principals) who can then make a decision whether to allow the mail through the system and/or whether to take appropriate action within the terms of this eSafety and Digital Technology Policy.

A student will be required to hand over his/her digital device and passcode to a member of staff if:

- there is a suspicion that the digital device has unsuitable material stored on it;
- a student has disrupted a lesson through improper use of a digital device;
- a student has misused his digital device, without staff permission, to take photographs/video;
- the digital device or any of its features has been used for any form of bullying;

- games are being played on the digital device during school hours;
- the digital device has been used to breach any school rule/policy and general well-being of staff and students.

2 *Sanctions*

If unsuitable material is found on any digital device, including cloud storage and email, it will be referred to the (Head of Year/Head of Department/Head of School/Vice Principal). Inappropriate use may result in access being withdrawn to digital services. Any student who refuses to cooperate or violates any aspect of this eSafety and Digital Technology Policy may face disciplinary action in line with the College's Stepped Consequences and Positive Behaviour Policy. Very serious breaches of eSafety may result in the matter being reported to the PSNI and or external agencies such as Gateway Children's Social Services.

3 *Rules Governing Student Use of Digital Technology*

1. Students are not permitted to use any digital devices in the College, except with the explicit permission of a member of staff.

(Continued overleaf)

Acceptable Use of Digital Technology *Students*

(Continued)

2. Students may bring mobile phones to school. These should generally be switched off and kept securely by the student. Students should only use phones in class under the direction of a staff member.
3. If a student is using a mobile phone when he should not be, the phone may be confiscated by a staff member and returned at the end of the day. If a student refuses to comply with this, the phone may be retained until a parent/ carer collects it.
4. The DE funded C2k Education Network is the primary Internet provider. Students may also access the Internet in the Creative Digital Hub under the direction of staff.
5. Students must not post any unsuitable material on any Google Classroom and any comments made must be directly connected to work. The teacher's guidance and direction with regard to Google Classroom must be followed at all times.
6. Students may not log on using another person's username.
7. If unsuitable material is encountered by a student, he must inform the staff member/IT Manager immediately. The staff member/ IT Manager will refer the matter to the Head of Year or the Designated Teacher for Child Protection as appropriate.
8. At all times students must only access online content which is directly linked to their school work.
9. Students must not attempt to bypass filtering or to access inappropriate or illegal material.
10. Students must not execute any program received in email or found on a web page except as directed by the IT Manager or a teacher.
11. Students must not install or download any program/ file except as directed by the IT Manager or a teacher.
12. Students must not engage in any illegal activity, use obscene or racist language or retrieve, send, copy or display offensive messages, pictures or videos.
13. Students must refrain from cyberbullying and adhere to College's Anti-Bullying and Positive Behaviour Policies.
14. Students must not post any content online or record any media which would bring discredit on the College.
15. Digital devices (with the exception of mobile phones) brought into school must only contain work files and no software programs or games. Digital devices containing programs or games may be confiscated. All portable storage devices should be regularly virus scanned.
16. Digital devices must not be used for unauthorised commercial purposes on College premises.
17. Students must not attempt to break passwords of other students or staff, or access any digital device apart from their own.
18. Students must not intentionally damage or modify any digital technology or use any software that can damage or override security.
19. Students must adopt good eSafety practice when using Digital Technology outside school and realise that the College's eSafety and Digital Technology Policy covers their actions outside school, if related to their membership of the school or involving any member of the school community.
20. Students must adhere to The Copyright, Designs and Patents Act.

St Malachy's College

Policy for the Acceptable Use of Digital Technology

Student Agreement

For completion by pupil:

I have read and understand the guidelines and conditions for appropriate use of Internet services in St Malachy's College. I understand that any violation of these conditions may result in withdrawal of privileges and disciplinary action.

I agree to report any misuse of the school system to a member of staff and report any access to inappropriate websites while using the school facilities to my Form Tutor or Head of Year.

Your Name (block capitals) Class

Signature

Appendix 4

eSafety *DE Circulars and Guidance*

DE Circular 2007/01 (18/06/07) - Acceptable Use of the Internet and Digital Technologies in Schools DE Circular 2011/22 (27/09/11) - Internet Safety

DE Circular 2013/25 (06/12/13) - eSafety Guidance

DE Letter (12/06/15) - General Advice to Everyone/General Advice to Parents

DE Circular 2016/26 (01/12/16) - Effective Educational Uses of Mobile Digital Devices DE Circular 2016/27 (01/12/16) - Online Safety

C2K Information Sheet ENO74 - Acceptable Use Policy for C2k Services

DE Circular 2017/04 (Updated 02/09/19) - Safeguarding/Child Protection - A Guide for Schools - Update DE Circular 2020/05 (05/06/20) - Guidance for Schools on Supporting Remote Learning

DE Circular 2021/01 (04/01/21) - Further Guidance for Schools on Supporting Remote Learning to Provide Educational Continuity

DE Circular Number 2021/25 (06/12/21) - Further Guidance for Schools on Supporting Remote Learning to Provide Educational Continuity