# Holy Cross and All Saint’s RC Primary School

## E-Safety Policy

**July 2024**

## Contents

Introduction ........................................................................................................3

Policy Governance ..............................................................................................4

E-Safety Education and Training .........................................................................9

Education & Training – Staff ...............................................................................9

Education and Training – Parents and Governors ................................................9

Communication devices and methods ..................................................................9

Unsuitable/inappropriate activities.....................................................................12

Good practice guidelines ..................................................................................15

Incident Management.........................................................................................22

Further information and support .......................................................................25

Appendix 1 – Student/Pupil AUP .......................................................................26

Appendix 2 – Staff, Volunteer, Community User AUP.........................................27

Appendix 3 - Details of school Firewall system……………………………………………………………37

## Introduction

This School E-Safety Policy Template is intended to help school leaders produce a suitable E-Safety policy document which will consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, Behaviour and Anti- Bullying policies.

The School E-Safety Policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

## Policy Governance

## Development, Monitoring and Review of this Policy

| Position | Name(s) |
|---|---|
| *School E-Safety Coordinator / Officer* | Ms Richardson |
| *Headteacher* | Mrs A Bell |
| *Teachers* | Mrs Randle and Ms Richardson |
| *Support Staff* | NA |
| *ICT Technical staff* | Computeam: Steven Williams |
| *Governors* | Mr E. Connolly |
| *Parents and Carers* | N/A |
| *Community users* | N/A |
| | |

## Schedule for Review

| | |
|---|---|
| This e-safety policy was approved by the | *Governing Body:* |
| The implementation of this e-safety policy will be monitored by: | *E-Safety Officer*<br>*Senior Leadership Team* |
| Monitoring will take place at regular intervals: | *Annually* |
| The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the e-safety policy generated by the monitoring group *(or named individual)* at regular intervals: | *Annually* |
| The E-Safety Policy will be reviewed *annually*, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | *Annually* |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | See *Incident Management Section* |

## Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

## Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

### Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

### Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community
- The Headteacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

### E-Safety Coordinator/Officer:

- leads the e-safety initiatives.
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to Senior Leadership Team

### Network Manager / Technical staff:

Salford City Council, with the support of *Computeam* are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack. This will be ensured by maintaining a robust firewall system which protects all users from malicious, dangerous or inappropriate content.

- that the school meets the e-safety technical requirements outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy

## Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the appropriate person, as defined in *Section 11*

Designated person(s) for Safeguarding

should be trained in e-safety issues and be aware of the potential for serious child Protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

## E-Safety Committee

Members of the E-safety will assist the E-Safety Coordinator/Officer with:

- the production, review and monitoring of the school e-safety policy

## Students/pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. In KS1, parents would sign on behalf of pupils; in KS2, pupils do this independently.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

## Parents/Carers

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student/Pupil Acceptable Use Policy
- accessing the school ICT systems or Learning Platform in accordance with the school Acceptable Use Policy.

## Community Users

Not applicable

## E-Safety Education and Training

### Education – students / pupils

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies.
- Students/pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- E-safety rules will displayed in all classrooms.
- A prominent display will be produced to remind pupils of the key messages of e-safety.

### Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- *A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process. All Staff will receive training as part of the school's annual safeguarding sessions.*
- *Sessions*
- *All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies*
- Training sessions for parents will take place regularly.

### Education and Training – Parents and Governors

It is essential that Governors and parents receive e-safety awareness and/or training and understand their responsibilities. Training will be offered as follows:

*As part of Salford LEA's Governor Training provision.*

## Communication devices and methods

The following table shows the school's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

| | Staff & other adults | | | | Students/Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| **Communication method or device** | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| | ☑ | ⚠ | ⚠ | ☒ | ☑ | ⚠ | ⚠ | ☒ |
| Mobile phones may be brought to school | † | | | | | | | † |
| Use of mobile phones in lessons (at Headteacher's discretion) | | † | | | | | | † |
| Use of mobile phones in social time | † | | | | | | | † |
| Taking photos or videos on personal mobile phones or other camera devices (providing a clear educational purpose is evident) | | † | | | | † | † | |
| Use of personal hand held devices eg PDAs, PSPs | † | | | | | | | † |
| Use of personal email addresses in school, or on school network | † | | | | | | † | |
| Use of school email for personal emails | † | | | | | | | † |
| Use of chat rooms / facilities | | † | | | | | † | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Use of instant messaging | | † | | | | | † | |
| Use of social networking sites | | † | | | | | | † |
| Use of blogs | | † | | | | | † | |

This table indicates when some of the methods or devices above may be allowed:

| | Circumstances when these may be allowed | |
|---|---|---|
| **Communication method or device** | **Staff & other adults** | **Students/Pupils** |
| Mobile phones may be brought to school | *N/A* | *Headteacher's permission* |
| Use of mobile phones in lessons | Clear education purpose i.e. *Tweeting / Blogging* | *N/A* |
| Use of mobile phones in social time | *during breaks or after school* | *N/A* |
| Taking photos on personal mobile phones or other camera devices | *N/A* | Headteacher's permission i.e. *residential trip* |
| Use of personal hand held devices eg PDAs, PSPs | *N/A* | *N/A* |
| Use of personal email addresses in school, or on school network | *Clear educational purpose* | *N/A* |
| Use of school email for personal emails | *Clear educational purpose* | *N/A* |
| Use of chat rooms / facilities | *Clear educational purpose* | *N/A* |
| Use of instant messaging | *Clear educational purpose* | *N/A* |
| Use of social networking sites | *Clear educational purpose* | *N/A* |
| Use of blogs | *Clear educational purpose* | *N/A* |
| | | |
| | | |

### *Unsuitable/inappropriate activities*

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

| | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|
| **User Actions** | ☑ | ⚠ | ⚠ | ☒ | ☒ |
| child sexual abuse images | | | | | ☒ |
| promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation | | | | | ☒ |
| adult material that potentially breaches the Obscene Publications Act in the UK | | | | | ☒ |
| criminally racist material in UK | | | | | ☒ |
| Pornography | | | | | ☒ |
| promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability | | | | | ☒ |
| promotion of racial or religious hatred | | | | | ☒ |
| threatening behaviour, including promotion of physical violence or mental harm | | | | | ☒ |
| any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | ☒ | |
| Using school systems to run a private business | | | | ☒ | |

| | | | | | |
|---|---|---|---|---|---|
| Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the school | | | | ☒ | |
| Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions | | | | ☒ | |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) | | | | ☒ | |
| Creating or propagating computer viruses or other harmful files | | | | ☒ | |
| Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet | | | | ☒ | |
| On-line gaming (educational) | | † | | | |
| On-line gaming (non educational) | | | | † | |
| On-line gambling | | | | † | |
| Accessing the internet for personal or social use (e.g. online shopping, banking etc) | † | | | | |
| File sharing e.g. music, films etc | | | | † | |
| Use of social networking sites | † | | | | |
| Use of video broadcasting eg Youtube | † | | | | |
| Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses) | † | | | | |

This table indicates when some of the methods or devices above may be allowed:

| | **Circumstances when these may be allowed** | |
|---|---|---|
| **User Actions** | **Staff & other adults** | **Students/Pupils** |
| On-line gaming (educational) | *Clear educational purpose* | *Clear educational purpose* |
| On-line gaming (non educational) | N/A | N/A |
| On-line gambling | N/A | N/A |
| Accessing the internet for personal or social use (e.g. online shopping, banking etc) | *During break or social times* | *Clear educational purpose* |
| File sharing e.g. music, films etc | N/A | N/A |
| Use of social networking sites | *Clear educational purpose* | |
| Use of video broadcasting eg Youtube | *Clear educational purpose* | *Clear educational purpose* |
| Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses) | File storage moved to Google Drive March 2022 to allow staff access at home. No use of USBs now needed.<br>School reports completed on Report Writer- cloud based and password protected. | *No* |

## Good practice guidelines

### Email

Best practice

☑ **DO**

Staff and students/pupils should only use their school email account to communicate with each other

Safe practice

⚠

Check the school e-safety policy regarding use of your school email or the internet for personal use e.g. shopping

Poor practice

☒ **DO NOT**

Staff: don't use your personal email account to communicate with students/pupils and their families without a manager's knowledge or permission – and in accordance with the e-safety policy.

## Images, photos and videos

Best practice

☑ DO

Only use school equipment for taking pictures and videos.

Ensure parental permission is in place.

Safe practice

⚠

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

☒ **DO NOT**

Don’t download images from organisation equipment to your own equipment.

Don’t use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don’t retain, copy or distribute images for your personal use.

## Internet

Best practice

☑ **DO**

Understand how to search safely online and how to report inappropriate content .

Safe practice

⚠

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Poor practice

**☒ DO NOT**

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

## Mobile phones

Best practice

☑ **DO**

*Staff: If you need to use a mobile phone while on school business (trips etc), the school will should provide equipment for you.*

*Make sure you know about inbuilt software/ facilities and switch off if appropriate.*

Safe practice

⚠

Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first

Poor practice

☒ **DO NOT**

Staff: Don’t use your own phone without the Headteacher/SLT knowledge or permission.

Don’t retain student/pupil/parental contact details for your personal use.

## Social networking (e.g. Facebook/ Twitter)

Best practice

☑ **DO**

If you have a personal account, regularly check all settings and make sure your security settings are not open access.

Ask family and friends to not post tagged images of you on their open access profiles.

Safe practice

⚠

Don’t accept people you don’t know as friends.

Be aware that belonging to a ‘group’ can allow access to your profile.

Poor practice

☒ **DO NOT**

Don’t have an open access profile that includes inappropriate personal information and images, photos or videos.

Staff:

- Don’t accept students/pupils or their parents as friends on your personal profile.
- Don’t accept ex-students/pupils users as friends.
- Don’t write inappropriate or indiscrete posts about colleagues, students/pupils or their parents.

## Webcams

Best practice

**☑ DO**

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Safe practice

⚠

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

**☒ DO NOT**

Don’t download images from organisation equipment to your own equipment.

Don’t use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don’t retain, copy or distribute images for your personal use.

## Incident Management

| **Incidents (students/pupils):** | Refer to class teacher | Refer to Head of Department / Head of Year / other | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg detention / exclusion |
|---|---|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities) | Case by Case basis: See *Behaviour Policy* | | | | | | | | |
| Unauthorised use of non-educational sites during lessons | | | | | | | | | |
| Unauthorised use of mobile phone/digital camera / other handheld device | | | | | | | | | |
| Unauthorised use of social networking/ instant messaging/personal email | | | | | | | | | |
| Unauthorised downloading or uploading of files | | | | | | | | | |
| Allowing others to access school network by sharing username and passwords | | | | | | | | | |
| Attempting to access or accessing the school network, using another student's/pupil's account | | | | | | | | | |
| Attempting to access or accessing the school network, using the account of a member of staff | | | | | | | | | |
| Corrupting or destroying the data of other users | | | | | | | | | |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | | | | | | | | | |
| Continued infringements of the above, following previous warnings or sanctions | | | | | | | | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | | | | | | | | |

| | |
|---|---|
| Using proxy sites or other means to subvert the school's filtering system | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | |
| Deliberately accessing or trying to access offensive or pornography | |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | |

| **Incidents (staff and community users):** | Refer to Head of Department / Head of | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering / security etc | Removal of network / internet access rights | Warning | Further sanction |
|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities) | Case by Case basis, in line with Staff Acceptable Usage Policy Appendix 2 & Staff Code of Conduct Policy | | | | | | |
| Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email | | | | | | | |
| Unauthorised downloading or uploading of files | | | | | | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | | | | | | | |
| Careless use of personal data eg holding or transferring data in an insecure manner | | | | | | | |
| Deliberate actions to breach data protection or network security rules | | | | | | | |
| Corrupting or destroying the data of other users or causing | | | | | | | |

| | |
|---|---|
| deliberate damage to hardware or software | |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils | |
| Actions which could compromise the staff member's professional standing | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | |
| Using proxy sites or other means to subvert the school's filtering system | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | |
| Deliberately accessing or trying to access offensive or pornographic material | |
| Breaching copyright or licensing regulations | |
| Continued infringements of the above, following previous warnings or sanctions | |

## Further information and support

**For a glossary of terms used in this document:**

http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf

**For e-Safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People:**

http://www.salford.gov.uk/d/e-Safety-Practice-Guidance.pdf

**R u cyber safe?**

**E-safety tips about how to stay safe online:**

http://www.salford.gov.uk/rucybersafe.htm

## Appendix 1 – Student/Pupil AUP

# Student/pupil Acceptable Use Policy Agreement Template

Student/Pupil Acceptable Use Policy Agreement
This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The school will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

Please make sure you read and understand the following ☑ **I WILL** and ☒ **I WILL NOT** statements. If there's anything you're not sure of, ask your teacher.

## ☑ I WILL:

- treat my username and password like my toothbrush – I will not share it, or try to use any other person's username and password
- immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- respect others' work and property and will not access, copy, remove or change any one else's files, without their knowledge and permission
- be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- only use my personal /external devices (USB devices etc) in school if I have permission
- understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- immediately report any damage or faults involving equipment or software, however this may have happened
- only use chat, instant messaging or blog sites with permission and at the times that are allowed

## ☒ I WILL NOT:

- try (unless I have permission) to make downloads or uploads from the Internet
- take or share images (pictures and videos) of anyone without their permission
- use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes
- attempt to install programmes of any type on a machine, or store programmes on a computer
- try to alter computer settings
- Use social media of which I am below the recommended age to use (i.e. *Facebook* below 13 etc – see attached guidelines)

## Appendix 2 – Staff, Volunteer, Community User AUP

# Staff, Volunteer and Community User Acceptable Use Policy Agreement Template

### School Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- that staff, volunteers and community users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- that staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff, volunteers and community users will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

### Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. This includes the usage of the device by any third-party.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

- I will be professional in my communications and actions when using school ICT systems.

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- Files will be stored on the Google Drive (these must not contain pupils personal data) the drive can be accessed at home and is password protected. You must not share your password with others.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / *twitter etc*) it will not be possible to identify by name, or other personal information, those who are featured. I will delete any images or videos on my personal device and not store them, or make copies of them, including on a cloud storage system.

- I will only use chat and social networking sites in school in accordance with the school's policies.

- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.

    - This includes my usage of social media (on any device). I will not be 'friends' with or 'follow' or 'interact' with any parent of a pupil within the school, including those who are still within the education system.

- I will set all of my social media accounts to 'private' settings and will support of the e-safety officer if unsure of how to do this.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (laptops/mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules in line with the School's E-Safety Policy set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Local Authority Personal Data Policy

- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

## Staff, Volunteer and Community User Acceptable Use Agreement Form

This form relates to the student/pupil Acceptable Use Policy (AUP), to which it is attached.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police. This will be at the discretion of the Headteacher.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

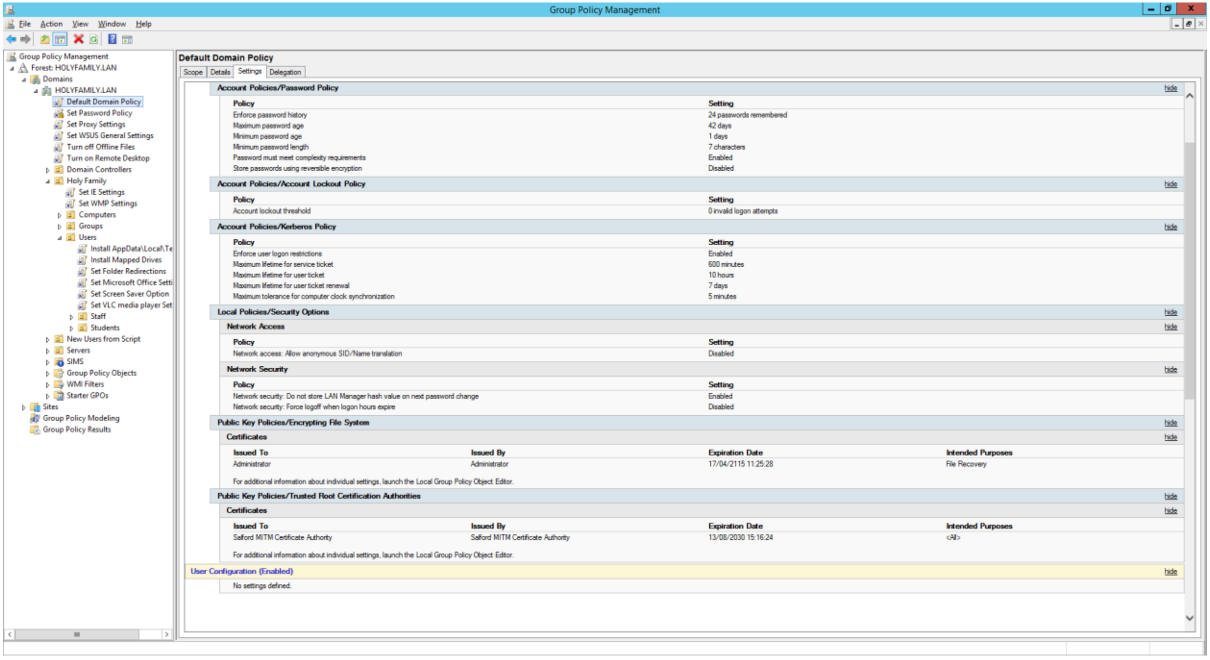
| | |
|---|---|
| Name | |
| Position | |
| Signed | |
| Date | |

## Appendix 3 – Firewall Details

All Salford City Council schools are Internet filtered by Smoothwall. Each site is configured identically.

### 1. Certificate

A Guardian Certificate supplied by SCC is delivered to ALL domain joined devices by Group Policy, added to the Default Domain Policy, see below.



Default Domain Policy

Account Policies/Password Policy

| Policy | Setting |
|---|---|
| Enforce password history | 24 passwords remembered |
| Maximum password age | 42 days |
| Minimum password age | 1 days |
| Minimum password length | 7 characters |
| Password must meet complexity requirements | Enabled |
| Store passwords using reversible encryption | Disabled |

Account Policies/Account Lockout Policy

| Policy | Setting |
|---|---|
| Account lockout threshold | 0 invalid logon attempts |

Account Policies/Kerberos Policy

| Policy | Setting |
|---|---|
| Enforce user logon restrictions | Enabled |
| Maximum lifetime for service ticket | 600 minutes |
| Maximum lifetime for user ticket | 10 hours |
| Maximum lifetime for user ticket renewal | 7 days |
| Maximum tolerance for computer clock synchronization | 5 minutes |

Local Policies/Security Options

Network Access

| Policy | Setting |
|---|---|
| Network access: Allow anonymous SID/Name translation | Disabled |

Network Security

| Policy | Setting |
|---|---|
| Network security: Do not store LAN Manager hash value on next password change | Enabled |
| Network security: Force logoff when logon hours expire | Disabled |

Public Key Policies/Encrypting File System

Certificates

| Issued To | Issued By | Expiration Date | Intended Purposes |
|---|---|---|---|
| Administrator | Administrator | 17/04/2115 11:25:28 | File Recovery |

For additional information about individual settings, launch the Local Group Policy Object Editor.

Public Key Policies/Trusted Root Certification Authorities

Certificates

| Issued To | Issued By | Expiration Date | Intended Purposes |
|---|---|---|---|
| Salford MITM Certificate Authority | Salford MITM Certificate Authority | 13/08/2030 15:16:24 | <All> |

For additional information about individual settings, launch the Local Group Policy Object Editor.

User Configuration (Enabled)

No settings defined.

All sites have a single Proxy set through Group Policy for Domain Joined Devices.

- Proxy address:10.5.192.30

There are several Port configurations dependent on the level of access required;

- Port: 8080 – KS1 – KS2
- Port: 8081 – KS3 – KS4
- Port: 8088 – KS5 – KS6
- Port: 9000 – Staff
- Port: 9090 – Domain Account Authentication

**Port: 9090** is the preferred port for Domain Joined devices, as Smoothwall determines the level of filtering from Active Directory for each user and also performs filtering reports down to user level.

For all none domain joined devices, it is advisable to set them up to correspond with the common user group of the device, i.e.

- Port: 8080 for all pupils in primary schools.
- Port: 9000 for all staff.

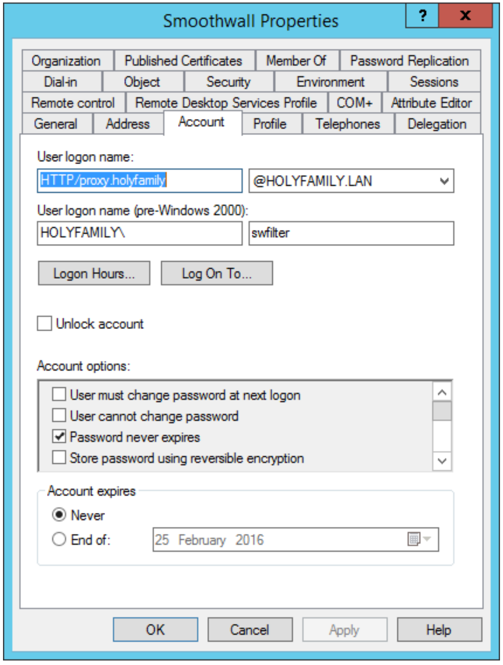
***Please note: The SCC Guardian Certificate will need to be installed manually on none domain joined devices.***

- Installing the certificate on iPads can be carried out by either manual installation via email or connecting to a PC and also via Apple Configurator for all managed devices.
- Android devices should be connected to a PC and the certificate copied to the local storage of the device and installed via the settings menu. Once installed, remove from local storage.
- Staff phones can have the certificate installed and this should be done via email to their device.

## 2. Smoothwall Domain Configuration

The site Domain is configured by Smoothwall to connect to the filtering framework. A username and password is created on the domain to access LDAP for authentication purposes (Fig.1). A further username and password is created (Fig.2) to access the Smoothwall Portal which is added to a created Security Group (Fig.3) for Smoothwall Portal Users.

Fig.1



User logon name:
HTTP/proxy.holyfamily @HOLYFAMILY.LAN

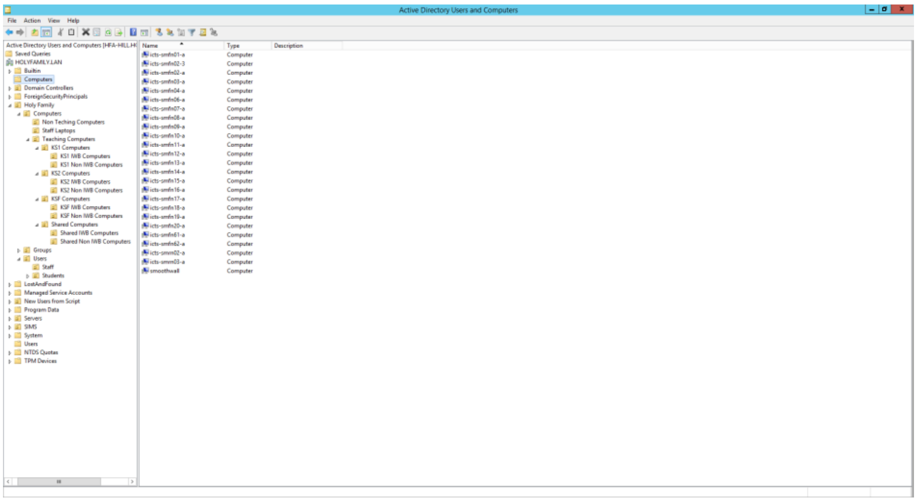
User logon name (pre-Windows 2000):
HOLYFAMILY\ swfilter

□ Unlock account

Account options:
□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

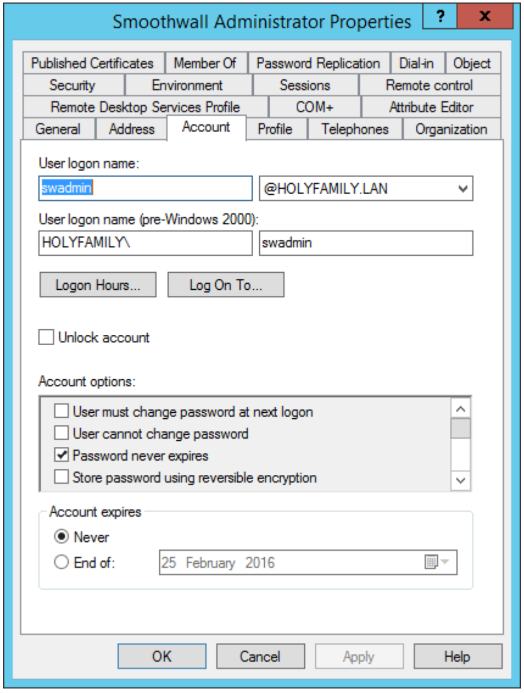
Account expires
● Never
○ End of: 25 February 2016

The user logon name is created by Smoothwall once Smoothwall has successfully configured the computer accounts in the domain, see below. (These must never be removed from the Computers container in Active Directory)



| Name | Type | Description |
|---|---|---|
| icts-smfn01-a | Computer | |
| icts-smfn02-3 | Computer | |
| icts-smfn02-a | Computer | |
| icts-smfn03-a | Computer | |
| icts-smfn04-a | Computer | |
| icts-smfn06-a | Computer | |
| icts-smfn07-a | Computer | |
| icts-smfn08-a | Computer | |
| icts-smfn09-a | Computer | |
| icts-smfn10-a | Computer | |
| icts-smfn11-a | Computer | |
| icts-smfn12-a | Computer | |
| icts-smfn13-a | Computer | |
| icts-smfn14-a | Computer | |
| icts-smfn15-a | Computer | |
| icts-smfn16-a | Computer | |
| icts-smfn17-a | Computer | |
| icts-smfn18-a | Computer | |
| icts-smfn19-a | Computer | |
| icts-smfn20-a | Computer | |
| icts-smfn61-a | Computer | |
| icts-smfn62-a | Computer | |
| icts-smmn02-a | Computer | |
| icts-smmn03-a | Computer | |
| smoothwall | Computer | |

Fig.2



User logon name:
swadmin @HOLYFAMILY.LAN

User logon name (pre-Windows 2000):
HOLYFAMILY\ swadmin

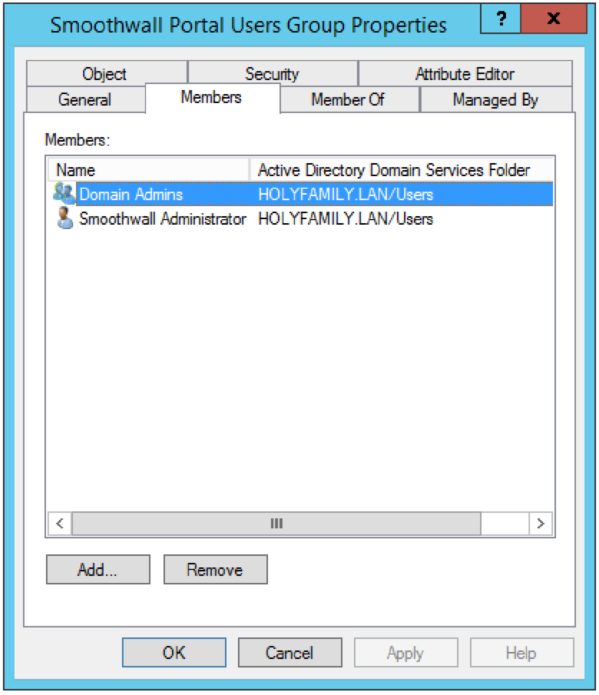
□ Unlock account

Account options:

- □ User must change password at next logon
- □ User cannot change password
- ☑ Password never expires
- □ Store password using reversible encryption

Account expires
- ● Never
- ○ End of: 25 February 2016

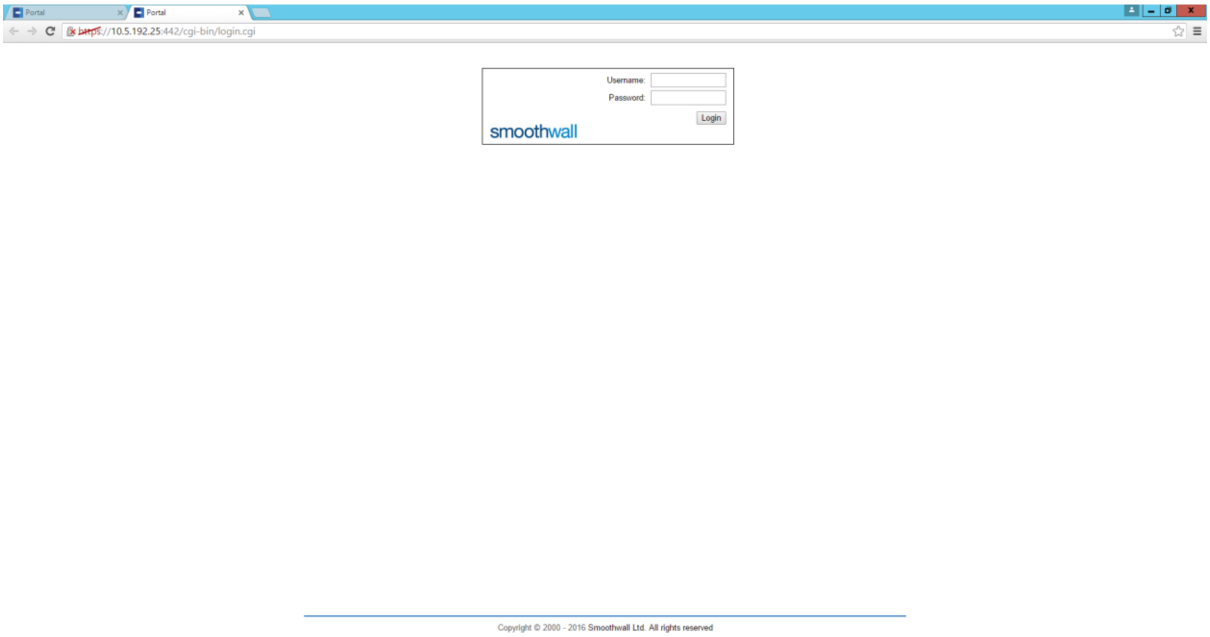
Fig.3



Members:

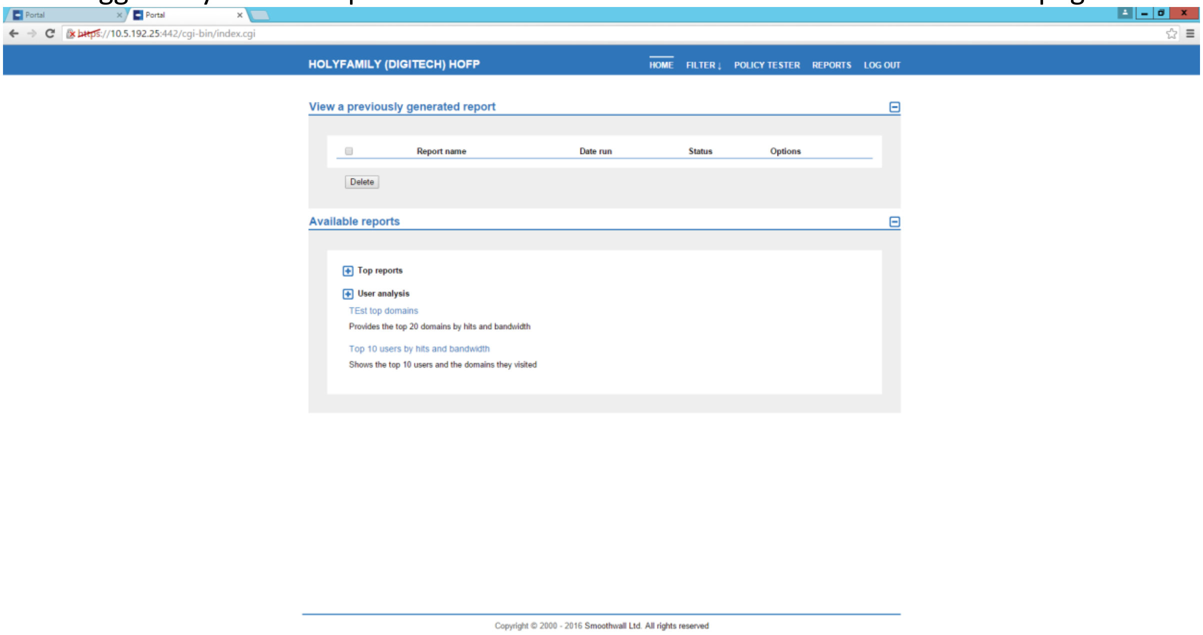
| Name | Active Directory Domain Services Folder |
|---|---|
| Domain Admins | HOLYFAMILY.LAN/Users |
| Smoothwall Administrator | HOLYFAMILY.LAN/Users |

The password for the Smoothwall Administrator (Username: swadmin) is the F1******* password. Again, these accounts must never be changed or removed from Active Directory. Access to the portal is via https://10.5.192.25:442/cgi-bin/login.cgi (this is the same for all sites). ***It is not accessible from outside of the SCC framework.***



Copyright © 2000 - 2016 Smoothwall Ltd. All rights reserved

Once logged in you will be presented with the Schools Smoothwall Portal home page.


Portal
Portal
https://10.5.192.25:442/cgi-bin/index.cgi
HOLYFAMILY (DIGITECH) HOFP
HOME
FILTER ↓
POLICY TESTER
REPORTS
LOG OUT
Delete

View a previously generated report

| □ | Report name | Date run | Status | Options |
|---|---|---|---|---|

Available reports

⊞ Top reports

⊞ User analysis

TEst top domains

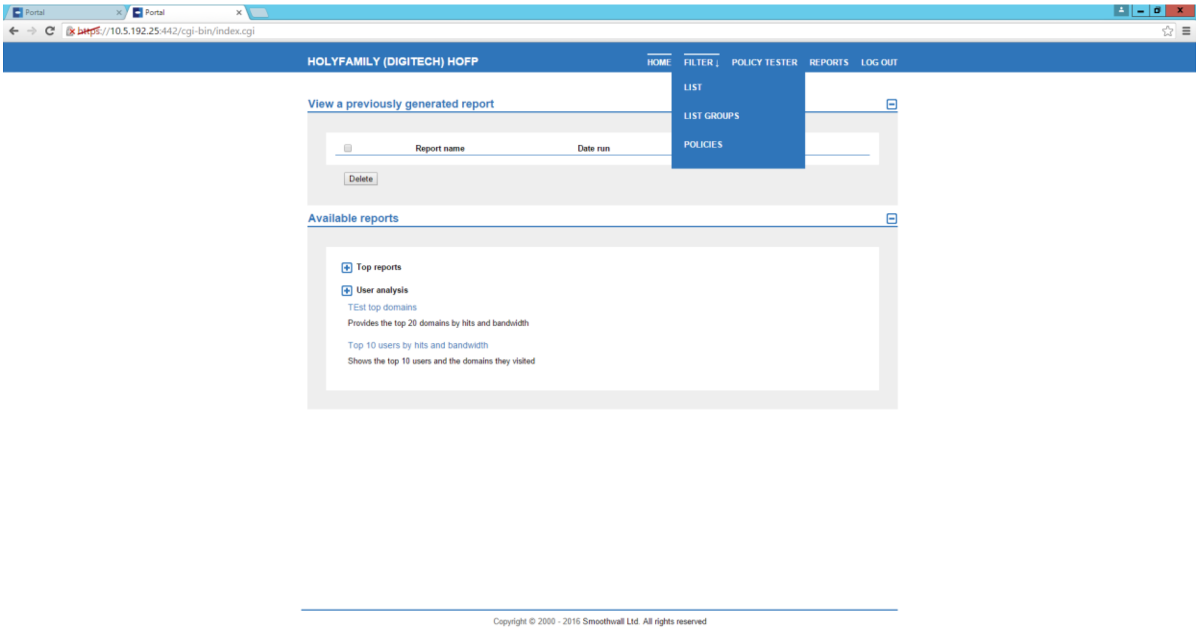
Provides the top 20 domains by hits and bandwidth

Top 10 users by hits and bandwidth

Shows the top 10 users and the domains they visited

Copyright © 2000 - 2016 Smoothwall Ltd. All rights reserved

The filter view has three categories



View a previously generated report

| □ | Report name | Date run |
|---|---|---|

Available reports

⊞ Top reports

⊞ User analysis

TEst top domains

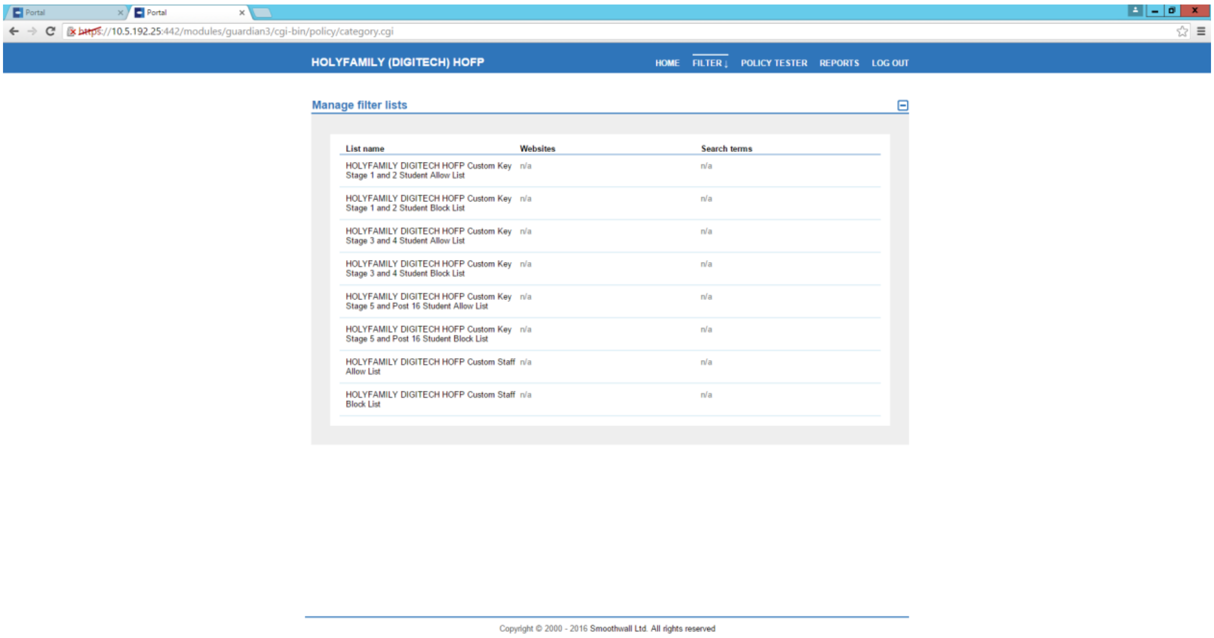
Provides the top 20 domains by hits and bandwidth

Top 10 users by hits and bandwidth

Shows the top 10 users and the domains they visited

Copyright © 2000 - 2016 Smoothwall Ltd. All rights reserved

## List View

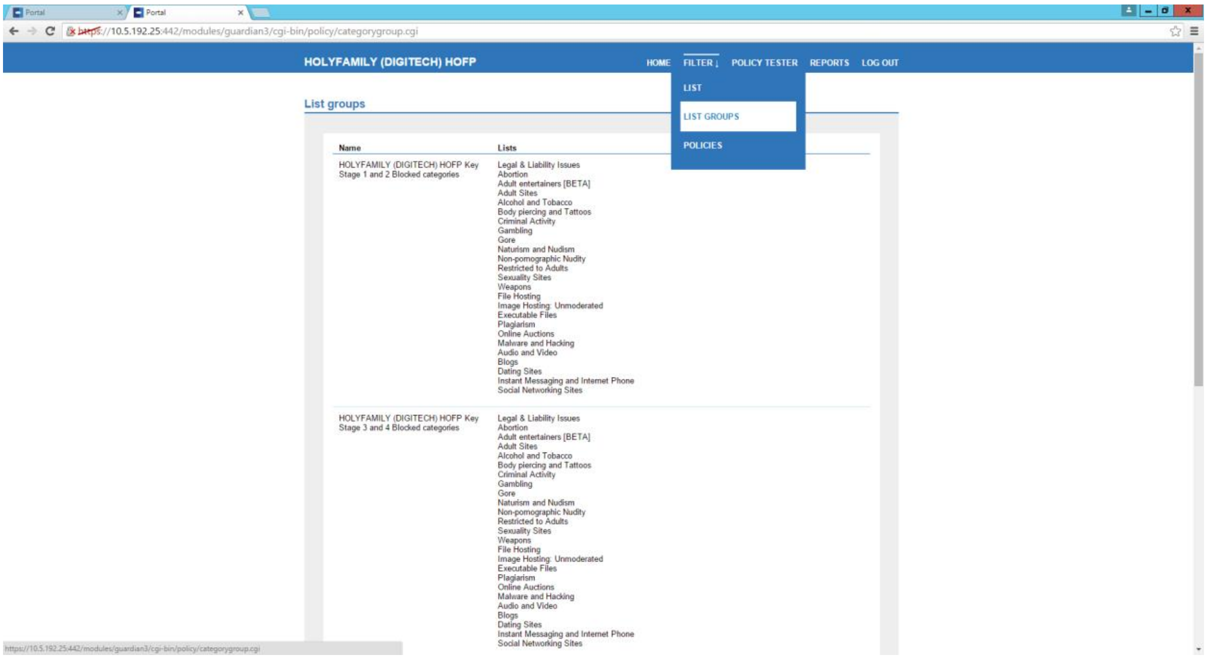

Portal
Portal
~~https~~://10.5.192.25:442/modules/guardian3/cgi-bin/policy/category.cgi
HOLYFAMILY (DIGITECH) HOFP
HOME
FILTER ↓
POLICY TESTER
REPORTS
LOG OUT

Manage filter lists

| List name | Websites | Search terms |
|---|---|---|
| HOLYFAMILY DIGITECH HOFP Custom Key Stage 1 and 2 Student Allow List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Key Stage 1 and 2 Student Block List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Key Stage 3 and 4 Student Allow List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Key Stage 3 and 4 Student Block List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Key Stage 5 and Post 16 Student Allow List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Key Stage 5 and Post 16 Student Block List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Staff Allow List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Staff Block List | n/a | n/a |

Copyright © 2000 - 2016 Smoothwall Ltd. All rights reserved

## List Groups

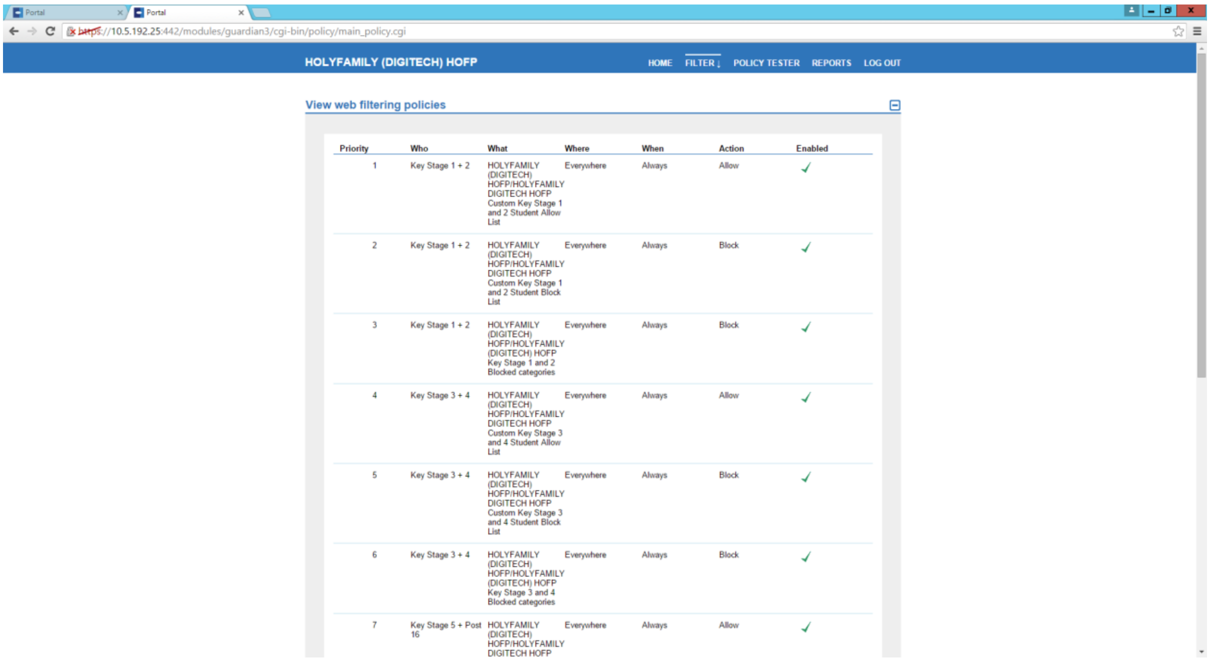

Portal
Portal
https://10.5.192.25:442/modules/guardian3/cgi-bin/policy/categorygroup.cgi
HOLYFAMILY (DIGITECH) HOFP
HOME
FILTER ↓
POLICY TESTER
REPORTS
LOG OUT
LIST
LIST GROUPS
POLICIES

List groups

| Name | Lists |
|---|---|
| HOLYFAMILY (DIGITECH) HOFP Key Stage 1 and 2 Blocked categories | Legal & Liability Issues<br>Abortion<br>Adult entertainers [BETA]<br>Adult Sites<br>Alcohol and Tobacco<br>Body piercing and Tattoos<br>Criminal Activity<br>Gambling<br>Gore<br>Naturism and Nudism<br>Non-pornographic Nudity<br>Restricted to Adults<br>Sexuality Sites<br>Weapons<br>File Hosting<br>Image Hosting: Unmoderated<br>Executable Files<br>Plagiarism<br>Online Auctions<br>Malware and Hacking<br>Audio and Video<br>Blogs<br>Dating Sites<br>Instant Messaging and Internet Phone<br>Social Networking Sites |
| HOLYFAMILY (DIGITECH) HOFP Key Stage 3 and 4 Blocked categories | Legal & Liability Issues<br>Abortion<br>Adult entertainers [BETA]<br>Adult Sites<br>Alcohol and Tobacco<br>Body piercing and Tattoos<br>Criminal Activity<br>Gambling<br>Gore<br>Naturism and Nudism<br>Non-pornographic Nudity<br>Restricted to Adults<br>Sexuality Sites<br>Weapons<br>File Hosting<br>Image Hosting: Unmoderated<br>Executable Files<br>Plagiarism<br>Online Auctions<br>Malware and Hacking<br>Audio and Video<br>Blogs<br>Dating Sites<br>Instant Messaging and Internet Phone<br>Social Networking Sites |

https://10.5.192.25:442/modules/guardian3/cgi-bin/policy/categorygroup.cgi

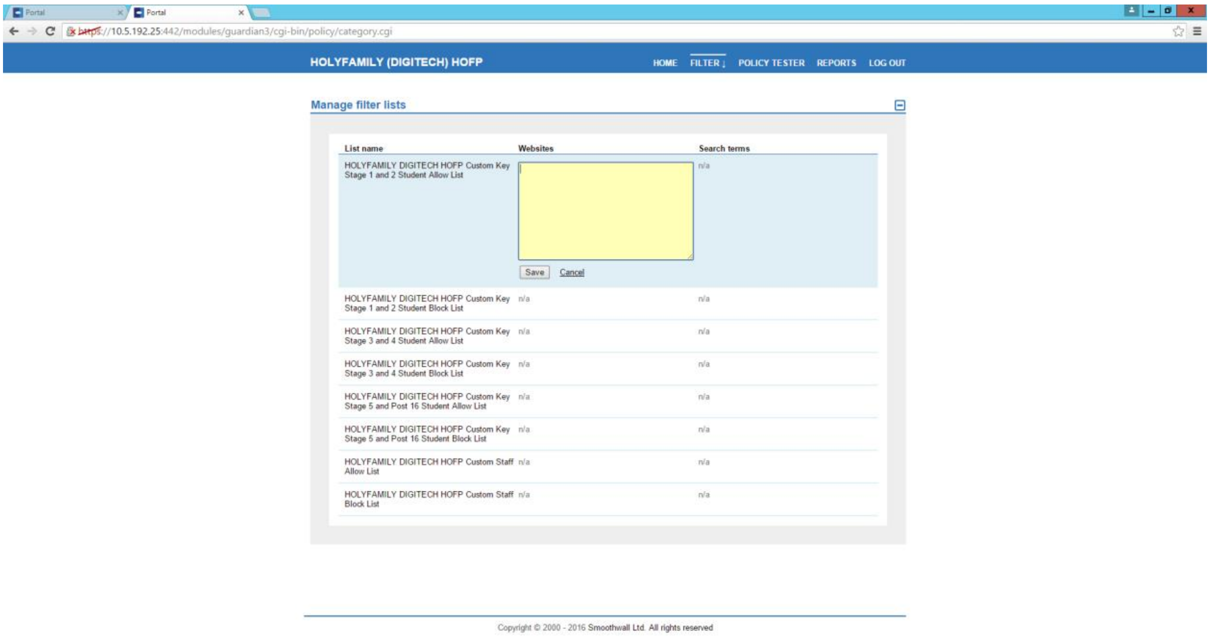
Policies


Portal
Portal
https://10.5.192.25:442/modules/guardian3/cgi-bin/policy/main_policy.cgi
HOLYFAMILY (DIGITECH) HOFP
HOME
FILTER ↓
POLICY TESTER
REPORTS
LOG OUT

View web filtering policies

| Priority | Who | What | Where | When | Action | Enabled |
|---|---|---|---|---|---|---|
| 1 | Key Stage 1 + 2 | HOLYFAMILY (DIGITECH) HOFP/HOLYFAMILY DIGITECH HOFP Custom Key Stage 1 and 2 Student Allow List | Everywhere | Always | Allow | ✓ |
| 2 | Key Stage 1 + 2 | HOLYFAMILY (DIGITECH) HOFP/HOLYFAMILY DIGITECH HOFP Custom Key Stage 1 and 2 Student Block List | Everywhere | Always | Block | ✓ |
| 3 | Key Stage 1 + 2 | HOLYFAMILY (DIGITECH) HOFP/HOLYFAMILY (DIGITECH) HOFP Key Stage 1 and 2 Blocked categories | Everywhere | Always | Block | ✓ |
| 4 | Key Stage 3 + 4 | HOLYFAMILY (DIGITECH) HOFP/HOLYFAMILY DIGITECH HOFP Custom Key Stage 3 and 4 Student Allow List | Everywhere | Always | Allow | ✓ |
| 5 | Key Stage 3 + 4 | HOLYFAMILY (DIGITECH) HOFP/HOLYFAMILY DIGITECH HOFP Custom Key Stage 3 and 4 Student Block List | Everywhere | Always | Block | ✓ |
| 6 | Key Stage 3 + 4 | HOLYFAMILY (DIGITECH) HOFP/HOLYFAMILY (DIGITECH) HOFP Key Stage 3 and 4 Blocked categories | Everywhere | Always | Block | ✓ |
| 7 | Key Stage 5 + Post 16 | HOLYFAMILY (DIGITECH) HOFP/HOLYFAMILY DIGITECH HOFP | Everywhere | Always | Allow | ✓ |

The Policies view is NOT editable.
List is where the exceptions are added for a specific group;


Portal
Portal
~~https~~://10.5.192.25:442/modules/guardian3/cgi-bin/policy/category.cgi
HOLYFAMILY (DIGITECH) HOFP
HOME
FILTER ↓
POLICY TESTER
REPORTS
LOG OUT
Save
Cancel

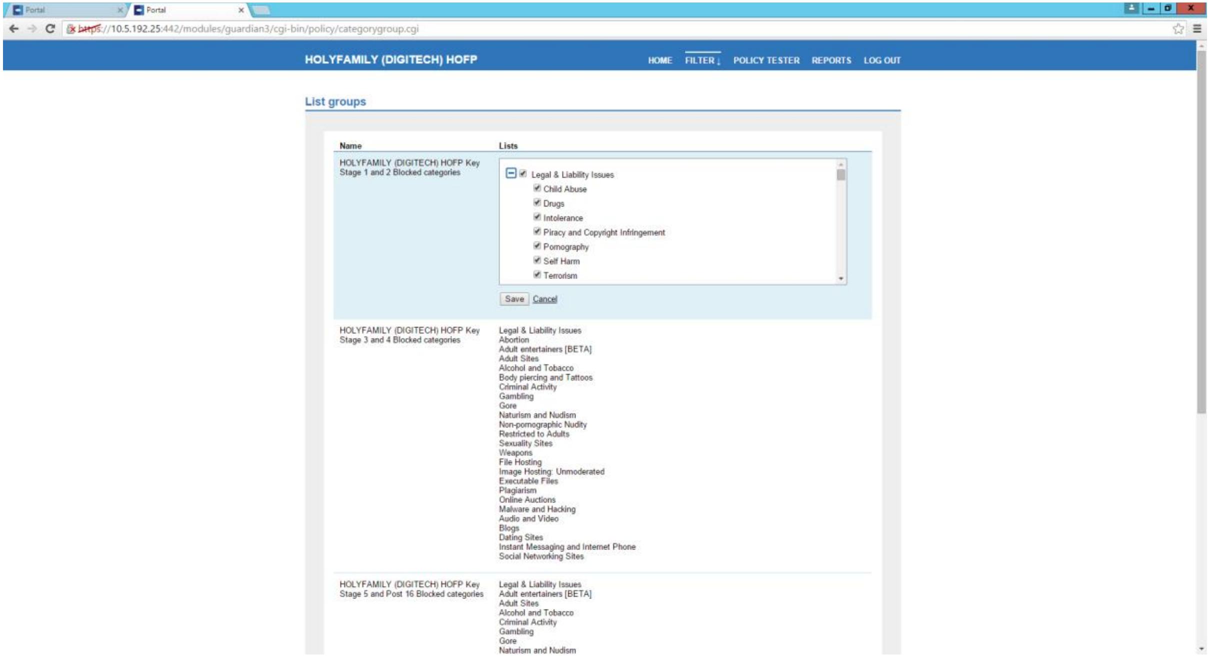
Manage filter lists

| List name | Websites | Search terms |
|---|---|---|
| HOLYFAMILY DIGITECH HOFP Custom Key Stage 1 and 2 Student Allow List |  | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Key Stage 1 and 2 Student Block List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Key Stage 3 and 4 Student Allow List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Key Stage 3 and 4 Student Block List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Key Stage 5 and Post 16 Student Allow List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Key Stage 5 and Post 16 Student Block List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Staff Allow List | n/a | n/a |
| HOLYFAMILY DIGITECH HOFP Custom Staff Block List | n/a | n/a |

Copyright © 2000 - 2016 Smoothwall Ltd. All rights reserved

Enter URL in box and Save changes. This can be for a group block or group allow.

The List Group is where global group default filters are applied or not;


Portal
Portal
~~https~~://10.5.192.25:442/modules/guardian3/cgi-bin/policy/categorygroup.cgi
HOLYFAMILY (DIGITECH) HOFP
HOME
FILTER ↓
POLICY TESTER
REPORTS
LOG OUT
Save
Cancel

List groups

| Name | Lists |
|---|---|
| HOLYFAMILY (DIGITECH) HOFP Key Stage 1 and 2 Blocked categories | ☑ Legal & Liability Issues<br>☑ Child Abuse<br>☑ Drugs<br>☑ Intolerance<br>☑ Piracy and Copyright Infringement<br>☑ Pornography<br>☑ Self Harm<br>☑ Terrorism |
| HOLYFAMILY (DIGITECH) HOFP Key Stage 3 and 4 Blocked categories | Legal & Liability Issues<br>Abortion<br>Adult entertainers [BETA]<br>Adult Sites<br>Alcohol and Tobacco<br>Body piercing and Tattoos<br>Criminal Activity<br>Gambling<br>Gore<br>Naturism and Nudism<br>Non-pornographic Nudity<br>Restricted to Adults<br>Sexuality Sites<br>Weapons<br>File Hosting<br>Image Hosting: Unmoderated<br>Executable Files<br>Plagiarism<br>Online Auctions<br>Malware and Hacking<br>Audio and Video<br>Blogs<br>Dating Sites<br>Instant Messaging and Internet Phone<br>Social Networking Sites |
| HOLYFAMILY (DIGITECH) HOFP Key Stage 5 and Post 16 Blocked categories | Legal & Liability Issues<br>Adult entertainers [BETA]<br>Adult Sites<br>Alcohol and Tobacco<br>Criminal Activity<br>Gambling<br>Gore<br>Naturism and Nudism |

Check or uncheck what is applicable to each site and Save changes.

*Please note: Once the changes have been made it can take up to 2 hours (approx.) to propagate the changes across all the Smoothwall servers.*

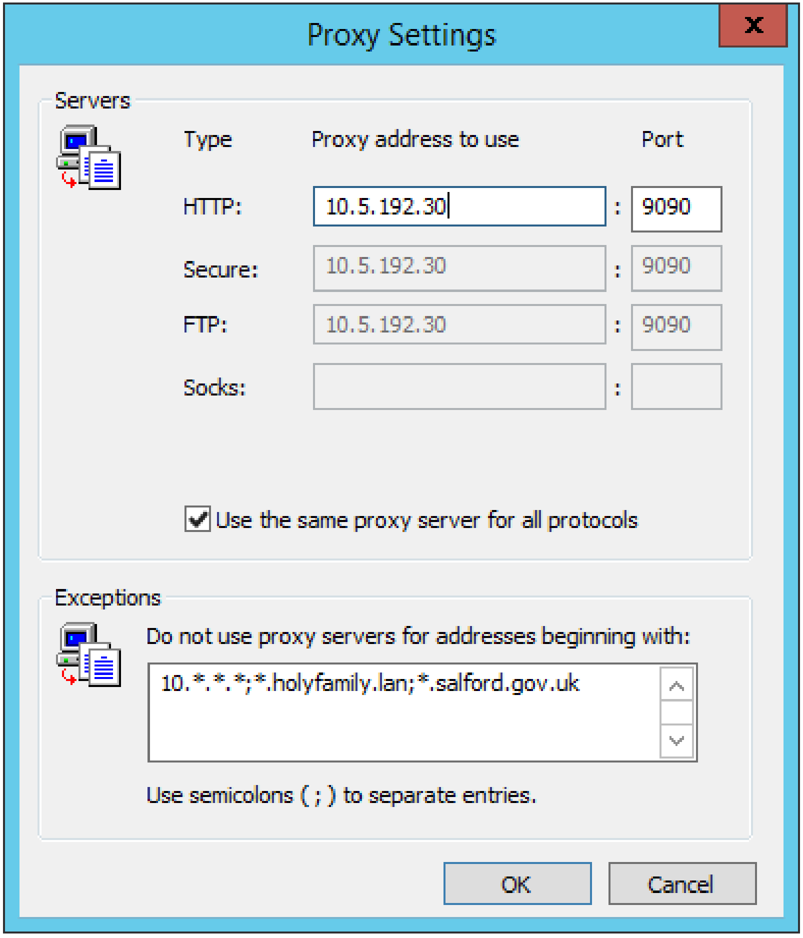
## 3. Proxy configuration on clients

As indicated earlier, all sites use a single proxy that is configured and delivered via group policy for domain joined devices and manually for none domain joined devices.
The standard configuration for all sites is shown below

- Proxy server: 10.5.192.30
- Port: 9090

Proxy exceptions are: 10.*.*.*;*.<local domain>;*.salford.gov.uk

Example:



Proxy Settings

Servers

| Type | Proxy address to use | Port |
|---|---|---|
| HTTP: | 10.5.192.30 | 9090 |
| Secure: | 10.5.192.30 | 9090 |
| FTP: | 10.5.192.30 | 9090 |
| Socks: | | |

☑ Use the same proxy server for all protocols

Exceptions

Do not use proxy servers for addresses beginning with:

10.*.*.*;*.holyfamily.lan;*.salford.gov.uk

Use semicolons ( ; ) to separate entries.

Any issues that arise with filtering, proxy errors and Internet connection issues should be directed to the SCC IT Service Desk – IT.ServiceDesk@salford.gov.uk for a resolution.