South West Grid for Learning Trust

SAFETY AND SECURITY
Introduction to Safety and Security

Safety and security is a prime consideration for all education establishments using the Internet and is represented by the umbrella concept of ‘SWGfL Safe’. The South West Grid for Learning (SWGfL) has invested significantly in both helping to reduce the online risks and encouraging healthy, safe and positive use of online and mobile technologies. This document details the policies, services, advice and support that SWGfL or its partners have developed or deployed.

The document contains key content and is divided into 3 sections as follows;

Policy and Leadership
At the heart of the SWGfL is the Acceptable Usage Policy that defines the purpose of and how the services should be used. The section also includes advice and guidance for institutions with managing issues that they may encounter. Finally the section also includes a summary of the Byron review that was published in March 2008 and commissioned by the Prime Minister.

Infrastructure Services
The section details the array of technical services and technologies that SWGfL uses to support and enable the service provision in line with the policy definition. Additionally the section provides administrative and user information for some of these services.

Education and Resources
This section is perhaps the most critical area that promotes and embeds positive and safe use of online and mobile technologies. The section includes information that signposts tried and tested resources and programmes for use with children and young people. Also included are details for parents and the parent programme that SWGfL is pioneering that is helping to bridge the digital divide. Further information on awareness sessions that SWGfL has developed are also included, all aimed at increasing the confidence of teachers and school staff to engage with children and young people with regards e safety. All these resources, programmes and training is aimed at helping communities across the South West to enjoy and embrace the new technologies in a safe and positive manner.
POLICY AND LEADERSHIP

Internet Acceptable Usage Policy
Procedure for Reviewing Internet Sites
The Internet Safety Protocol
The Byron Review
SWGfL Internet Acceptable Usage Policy

Introduction
The purpose of this policy is to ensure that users of the South West Grid for Learning (SWGfL) understand the way in which the Internet is to be used. The policy aims to ensure that the Internet is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk. Users should read this policy alongside the other SWGfL policies: the Filtering Policy and the Email Policy.

Scope
The policy applies to all users and administrators of the SWGfL services and/or infrastructure. On evidence provided by the SWGfL, an employee may be disciplined by their employer. At the same time, if a user's conduct and/or action(s) are illegal, the user may become personally liable in some circumstances.

Policy statement
The SWGfL encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. It should not compromise the SWGfL’s information and computer systems nor have the potential to damage the SWGfL's reputation.

Please read this policy carefully as you will be deemed to be aware of its contents.

Use of Internet facilities
The SWGfL expects all users to use the Internet responsibly and strictly according to the following conditions: For the purposes of this document, Internet usage means any connection to the Internet via Web browsing, external email or news groups.

Users shall not visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- any other information which may be offensive to colleagues.

SWGfL acknowledges that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use (for example investigating racial issues). Any such access should be preplanned and recorded so that it can be justified if required.

Incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following material will be reported to the police:
- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
• adult material that potentially breaches the Obscene Publications Act in the UK
• criminally racist material in the UK.

If inappropriate material is accessed accidentally, users should immediately report this to the SWGfL so that this can be taken into account in monitoring.

• Use the SWGfL facilities for running a private business
• Enter into any personal transaction that involves the SWGfL or member Local Authorities in any way
• Visit sites that might be defamatory or incur liability on the part of the SWGfL or member Local Authorities or adversely impact on the image of the SWGfL
• Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of the SWGfL, or to the SWGfL itself
• Reveal or publicise confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships
• Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet
• Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.

Monitoring

The SWGfL will monitor and audit the use of the Internet to see whether users are complying with the policy. Any potential misuse identified by the SWGfL will be reported to the connected establishment and/or relevant organisation.
Procedure for Reviewing Internet Sites for Suspected Harassment and Distress

This guidance has been prepared by the South West Grid for Learning (SWGfL) and Avon and Somerset Police in conjunction with each of the local constabularies to SWGfL (Devon and Cornwall, Dorset, Gloucestershire and Wiltshire). This guidance integrates with the SWGfL Acceptable Usage Policy and is intended for use when schools need to investigate incidents within schools that involve the use of web based services, such as on-line bullying. The procedure described below will ensure that schools are following best practice to conduct an investigation in a safe and secure manner both for the school and any investigating member of staff.

A growing number of web sites are being used by pupils outside of the school that allow them to communicate with their peers: Bebo, MySpace, You Tube, MSN Spaces are examples of many such sites. The generic term for them is “Web 2.0” technologies and they allow anyone to be able to publish information and communicate on the Internet. This can include short film clips (You Tube), personal information (Facebook), categorised by school (Bebo), and Chat forums (Habbo). Most students use them well and responsibly and indeed they can inspire creativity. However they can be, and are, misused at times. Misuse (for the purposes of this guidance) is categorised by the posting of text and images to such websites or services that cause distress and harassment to another individual. This relates to three particular areas of the law:

- Harassment (2 or more attempts) 
- Anti social behaviour
- Deception

When a school may have cause to investigate possible misuse:

- Images of a pupil (or member of staff) have been uploaded against their wishes and are causing harassment and/or distress.
- A web site has had comments added about another pupil / member of staff that are causing harassment and/or distress.
- Electronic information has been removed from the school for misleading purposes.

*Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case contact the police immediately.*

Web sites and specific page content that a school would like filtered can be reported to SWGfL for action.

---

1 Public Order Act 1986 (1994) Part 4a “Harassment, alarm or distress”
2 Computer Misuse Act (1990): “unlawful access of data, unlawful modification of data.”
Policy and Leadership

Please follow all steps in this procedure:

**More than one investigating member of staff**

Two senior colleagues from the school are required to be present (ideally this will be one male and female, of which one will be responsible for Child Protection within the school). This is vital to protect individuals if accusations are subsequently reported.

**Use a designated computer or device**

Conduct the investigation using a designated computer that will not be used by pupils and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the investigation.

**Ensure investigators have the necessary access**

The school’s network manager will need to set-up a “Staff Proxy” account. The SWGfL Managed Service team will be able to help if support is required for the creation of this account and can be contacted on 0870 9081708. This will enable one of the colleagues reviewing the sites to be able to access all Internet content without the SWGfL filtering service blocking access. The Staff Proxy will also record the addresses, time and dates of the sites reviewed to provide further protection. Access will be password protected and time limited.

**Report and Record**

During this process, if a reported site is confirmed to contain the alleged misuse please copy and paste the URL of the pages containing the content. To do this, click once on the address at the top of the page, then right click and choose “Copy”

Paste this address into the appropriate section on the form overleaf and then describe the nature of the content causing concern. It is important that all fields are completed and signatures attached to protect the individuals involved.

**Consideration and judgement**

Once this has been completed and fully investigated the school will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following

- Internal response or discipline procedures
- Local Authority involvement, support and/or discipline procedures
- Police (School or Neighbourhood) involvement and/or action

*If content being investigated includes images of Child abuse* then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- *incidents of ‘grooming’ behaviour*
- *the sending of obscene materials to a child*

*If this occurs isolate the computer in question, pulling the power from the unit, (i.e. the cable out of the back, take the battery from the laptop etc). Secure the unit by placing it in a locked cupboard etc.*

It is important that all of the above steps are taken as they will provide an evidence trail for the school, possibly the police and demonstrate that the sites visited were done for child protection needs. The completed form should be retained by school for evidence and reference purposes.

---

3 Sexual abuse involves for awareness of what is happening. The activities may involve physical contact, including penetrative (e.g. rape, buggery or oral sex) or non-penetrative acts. They may include n activities, or encouraging children to behave in sexually inappropriate ways. This includes nudity under 18 years of age.

4 Sexual Offence y for him to make the photograph proceedings, in any part of the world,"
Public Order Act 1986 (1994) Part 4a Harassment, alarm or distress

(1) A person is guilty of an offence if he causes threatening, abusive or insulting words or behaviour, or disorderly behaviour, or displays any writing, sign or other visible representation which is threatening, abusive or insulting, within the hearing or sight of a person likely to be caused harassment, alarm or distress thereby.

Computer Misuse Act (1990) creates three criminal offences:

Unauthorised access to computer material
This makes it illegal to access a computing system unless authorised to do so. As such it makes the activity of “hacking” a crime. It does not matter whether the hacker is remote, working from a distance over the remote area networks, or local, where persons such as employees or students who may have limited authorisation to use the computers but they knowingly exceed that authority. The hacking need not be directed at a particular computer, program or data. For example, it is unlawful, without proper authority: to use another person’s ID and password in order to access a computer, use data or run a program; to alter, delete, copy, or move a program or data, or simply to output a program or data; or to lay a trap to obtain a password.

Unauthorised access to a computer system with intent to commit or facilitate the commission of a further offence
This covers the situation where unauthorised access is gained with intent to commit a further offence. For example, a person may gain unauthorised access to a computer via another person’s ID in order to transmit offensive material.

Unauthorised modification of computer material
This offence includes the deliberate deletion or corruption of programs or data. It also includes the introduction of viruses etc., where these result in the modification or destruction of data.

The first of these three offences would most likely be dealt with in a magistrates court, but the other two are considered to be serious and would be referred to the Crown court where very large fines and/or gaol sentences are possible.
# Internet Harassment

<table>
<thead>
<tr>
<th>School</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>Reason for Investigation</td>
<td></td>
</tr>
</tbody>
</table>

## Primary Investigating Witness

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>

## Secondary Investigating Witness

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>

**Name and location of computer used for investigation**

**Web site(s) address**

<table>
<thead>
<tr>
<th>Reason why content is causing concern</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Conclusion and Action proposed or taken**
The Internet Safety Protocol

Safety and security is at the heart of the South West Grid for Learning (SWGfL) values. The following Internet Safety Protocol is designed to be a point of reference in the event that the Internet is used to access (or suspicion of access) inappropriate or illegal material.

Working in partnership with Avon and Somerset Police, the SWGfL Internet Safety working group has produced this document and is evidence of the considerable resources that have been invested in reducing the risks associated with the Internet.

As these situations only occur rarely, when they do arise, this compounds the issue and often leads to a stressful time. This document is aimed at providing quick and easy points of contact based on the attributes of the event (as detailed in the flow diagram).

The SWGfL is often required to provide supporting information in this type of situation. As a result of the legal position, the SWGfL has internal processes and procedures that will bring structure that enables information to be provided swiftly whilst adhering to relevant laws. This structure may also help to defuse the tension that can be associated with these situations.

Be assured that the SWGfL will manage any such situation both in, and with, confidence.
The Byron Review
Key Points for Schools

SWGfL has summarised key comments and recommendations for schools made by Dr Tanya Byron in her independent review; Safer Children in a Digital World published on 27th March 2008. It concludes with how SWGfL e-safety work can support South West schools in this respect.

This summary should be read in conjunction with the executive summary and full report. They can be downloaded at [http://www.dfes.gov.uk/byronreview/](http://www.dfes.gov.uk/byronreview/)

“One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area.”

The Byron review uses a useful analogy of how the risks are managed at public swimming pools. “Here we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim.” It goes on “however, overall, schools approach to e-safety and related support is neither coherent, comprehensive, nor consistent”

In relation to schools, the Byron review recommends that in good schools all staff will have a role with regards to e safety.

That in all schools, action is taken at a whole school level to ensure that e-safety is mainstreamed throughout the school’s teaching, learning and other practices. In particular I recommend that:

- Government should encourage schools to use Becta’s self review framework assessment to drive continual improvement in schools’ use of ICT including with regard to e-safety.
- 100% of schools should have Acceptable Use Policies that are regularly reviewed, monitored and agreed with parents and students. Guidance on this should be incorporated in Becta’s revised self review framework.
- that all schools and local children’s services use an accredited filtering service.

That the Government takes this opportunity to encourage school leaders and teachers to focus on e-safety by identifying it as a national priority for continuous professional development (CPD) of teachers and the wider school workforce. That all adults that work with particularly vulnerable children need to be familiar with the broad spectrum of online risks facing children, how they can support and empower children and young people to address them.

Ofsted take steps to hold schools to account and provide Government with a detailed picture of schools performance on e-safety. In particular I recommend that:

- Ofsted provide the Government with a snap shot report on school responses to question 4b of the SEF (regarding e-safety) by summer 2008.
- Ofsted should comment on the state of internet safety training in schools as part of its forthcoming long report on ICT due for publication in 2008.
If by 2011 evidence indicates widespread concerns in relation to school delivery of e-safety I recommend that Ofsted consider an assessment on performance in regard to e-safety in all school inspection reports.

In relation to extended schools and parents, the review comments:

- Parents also have a key role to play in managing children’s access to such material
- Parents either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”.

Supporting the delivery of e-safety skills through extended schools, the review then recommends:

- That schools to offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues

When talking about the family, the report suggests that this should extend beyond simply parents and carers:

- “Messages to the public around e-safety should be targeted towards grandparents and other relatives as well as parents.”

There will need to be sustainable education and children’s services initiatives to improve the skills of children and their parents around e-safety.

Concluding comments

To ignore e-safety issues when implementing the Every Child Matters agenda would be a major oversight and would ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable.

Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone’s responsibility to keep children safe in the non-digital world.

SWGfL: How it can help and what it is doing on your behalf

SWGfL applauds the publication of Dr Tanya Byron’s review and that it sets a clear statement that Local Authorities and schools have a fundamental role and responsibility for ensuring the safety of children when online, wherever they may be.

SWGfL has worked with its partners, local authorities and schools to help to make children safer when online. Many recommendations made by the review are already in action or progress across the South West. The SWGfL is able to help schools implement the recommendations made by Dr Byron’s review in the following ways:

- SWGfL provides safety and security services and is an accredited service by Becta
- SWGfL works closely with the regional police forces and child protection agencies
- SWGfL organises e-safety conferences for teachers and child protection professionals
- SWGfL provides reactive support for schools with e-safety issues or situations
- SWGfL is delivering e-safety sessions for parents, with the objective of offering the opportunity to all South West parents to attend such a session on a sustainable basis
- SWGfL is able to work alongside your school to support the delivery of e-safety related messages and programmes to your staff, pupils and communities.
- SWGfL commissions and conducts surveys and reports on all aspects of e-safety to help inform local, regional and national strategies.
INFRASTRUCTURE SERVICES

Internet Filtering Policy
Security Policy
Filtering Services
Filtering List Additions
Filtering Service Developments
Dealing with Proxy Bypass Web Sites
SWGfL Internet Filtering Policy

Introduction
Safety and Security lay at the heart of SWGfL services and the online access that SWGfL delivers across South West schools. Filtering is a founding service that is designed to filter out material found to be inappropriate for use in the education environment. Items that infringe SWGfL’s filtering policy are blocked. RM as managed service provider to SWGfL, provides the filtering service. SWGfL Filtering is powered by RM SafetyNet Plus.

This document summarises methods used to minimise the risks associated with accessing unsuitable and illegal web sites, and our filtering policy designed to help protect against these risks. The document outlines the categories that we filter and provides descriptions of the content deemed inappropriate in each of these categories.

In summary the categories included are:
- IWF Child Abuse Images database
- Pornography and illegal or age-restricted activity
- Drugs and substance abuse
- Violence
- Intolerance
- Web-based chat
- Web-based Social Networking
- Proxy Bypass
- Web-based mail services
- Mobile Phones/SMS/Ring Tones
- Non-educational games
- .MP3 and .exe files

More information on these categories is provided by this policy document.

Intelligence from industry blacklists, plus our dedicated filtering experts and web analysis techniques, and – importantly – input from establishments, Local Authorities and Regional Broadband Consortia, are used to build our unique database for education.

We welcome comments on this policy at any time via our email address: filtering@swgfl.org.uk

Content
Use of the Internet in education 2
Minimising the risks 2
SWGfL Filtering Internet filtering policy 4
Your Input 5
How to report inappropriate web sites 5
Further information and advice 5
Filter Category Definitions 6
Category availability matrix 8
Use of the Internet in education

93% of Internet users utilise the Internet as a fast and efficient means for gaining information (OxIS, 2007).

It has been proven to “promote effective learning. Students with Internet access have been shown to produce better-researched, more effective and well-presented projects” (Becta, 2007).

Despite the benefits 96% of Internet users believe that there should be restrictions in online content for children (OxIS, 2007).

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 (Becta, 2007).

The key Internet content risks have been categorised by Becta. These categories are outlined in the table below:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exposure to inappropriate materials</td>
<td>Material that is pornographic, hateful or violent in nature or encourages activities that are dangerous or illegal.</td>
</tr>
<tr>
<td>Inappropriate or illegal behaviour</td>
<td>Just as in the real world young people may get involved in inappropriate, antisocial or illegal behaviour while using new technologies. For example online bullying.</td>
</tr>
<tr>
<td>Copyright infringement</td>
<td>This could include downloading copyrighted material such as music files, or copying others’ homework.</td>
</tr>
<tr>
<td>Obsessive use of the Internet and ICT</td>
<td>This could lead to deterioration in the quality of schoolwork or negative impacts upon family relationships.</td>
</tr>
<tr>
<td>Physical danger and sexual abuse</td>
<td>This would include paedophiles using Internet chat rooms to target and develop relationships with young people for the sole purpose of sexual activity.</td>
</tr>
<tr>
<td>Inappropriate or illegal behaviour by school staff</td>
<td>This could include viewing or circulating inappropriate material.</td>
</tr>
</tbody>
</table>

Minimising the risks

By utilising SWGfL Filtering you have already significantly minimised the risks.

Between March 2007 and March 2008 we identified and blocked 2.9 billion attempts to access web sites that we know to contain offensive material. These web sites include both unsuitable and illegal material that would otherwise have been accessed, either inadvertently or by intent.

However, since the content on the web changes so dynamically it is simply not possible for any system based on exclusion to be 100% effective. It is important to understand that filtering is one element in a larger strategy for e-safety and acceptable use.
Becta highlight this point stating that “no technological solution can be 100 per cent effective in guaranteeing safety when using the internet and related technologies”. Becta advise that that “technology can help to minimise the risks to pupils, particularly when supported by a clear acceptable-use policy and appropriate e-safety education.” This coordinated approach is illustrated below.

SWGfL recommends that the following measures are adopted and used in conjunction with filtering:

- E Safety educational resources and programmes delivered across the whole school community (pupils, staff and parents)
- Appropriate supervision and e-safety education
- Creation and whole-school agreement of clearly defined, agreed and respected e safety and acceptable usage policy

The combination of these measures provides more complete protection.
SWGfL Internet filtering policy

SWGfL Filtering is designed to filter out material found to be inappropriate for use in the education environment. Items that infringe SWGfL's filtering policy are blocked by our filtering service.

SWGfL Filtering is customisable offering the ability to tailor your filtering solution in line with your establishment or regions Acceptable Use Policy. Using this solution it is possible to add to and also to override some of the sites that are filtered by SWGfL. The following is a list of categories that breach SWGfL's filtering policy. These categories are designed to act as a guide and not an exhaustive list:

<table>
<thead>
<tr>
<th>Filter list</th>
<th>Explanation and examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>IWF Illegal Images database</td>
<td>Sites which the Internet Watch Foundation has identified as breaching UK law</td>
</tr>
<tr>
<td>Pornography and illegal or age-restricted activity</td>
<td>Sexually explicit material including video or images as well as explicit animation and textual descriptions and sites promoting illegal or age-restricted activities</td>
</tr>
<tr>
<td>Drugs and substance abuse</td>
<td>Web sites that promote the use, manufacture, and distribution of illegal drugs, as well as sites which promote the abuse of legal substances such as prescription drugs, or the sale of alcohol to minors</td>
</tr>
<tr>
<td>Violence</td>
<td>Graphical portrayal of violence as well as sites which promote violence, or self endangerment. Instructions for making bombs and weapons</td>
</tr>
<tr>
<td>Intolerance</td>
<td>Material that promotes intolerance on the basis of religion, race, gender, or sexual orientation</td>
</tr>
<tr>
<td>Web-based chat</td>
<td>Web-based interactive chat and instant messaging that allow users to make unsolicited contact with individuals in the outside world without providing sufficient safeguards and protection to young people</td>
</tr>
<tr>
<td>Web-based Social Networking</td>
<td>Web-based social networking that allows users to make unsolicited contact with individuals in the outside world without providing sufficient safeguards and protection to young people.</td>
</tr>
<tr>
<td>Proxy Bypass</td>
<td>Sites that are designed to provide a route for bypassing Internet filters</td>
</tr>
<tr>
<td>Web-based email services</td>
<td>Web sites which allow access to free Web-based email services</td>
</tr>
<tr>
<td>Mobile Phones/SMS/Ring Tones</td>
<td>Mobile phone manufacturers, service operators, Web sites offering Internet based SMS/text messaging services and Web sites offering ring tones and phone logos</td>
</tr>
<tr>
<td>.MP3 and .exe files</td>
<td>Sites which provide .MP3 and .exe files used regularly by children for non-educational purposes</td>
</tr>
<tr>
<td>Non-educational games</td>
<td>Sites which provide or discuss games used regularly by children for non-educational purposes</td>
</tr>
</tbody>
</table>

Please note that material designed to educate, for example on matters such as sexual health or combating drug and substance abuse, would not normally contravene SWGfL's Internet filtering policy.

A general benchmark used by SWGfL to determine whether a site or part of a site should be filtered, is whether or not the questionable material is something which the national press may publish. If it is, then it is unlikely that SWGfL would choose to filter it.
Infrastructure Services

Not a 100% Guarantee
We proactively conduct thorough searches in an effort to block user access to any inappropriate material. However, it is important to understand that we are unable to offer a 100 per cent guarantee in providing an environment that is perceived to be ‘safe’ by everyone. One reason for this is the constantly changing nature and content of the World Wide Web.

SWGfL block user-access to a large number of unsuitable sites. We do this by the exclusive method, which means that when an inappropriate site is found, SWGfL prevents user access to it. This is in contrast to the inclusive method, which restricts access to all sites, except those identified as appropriate.

Although it is impossible to identify all unsuitable sites, we still believe that the exclusive method is the most suitable Internet filtering policy. Essentially, we believe that the majority of our customers would find the inclusive method too restrictive, as the scope of acceptable sites would be too limiting.

SWGfL Filtering dynamically scans individual web pages for inappropriate content as they are requested. This additional protection checks the suitability of pages that have not yet been added to a filter list, providing an additional safety measure which instantly adapts to unsuitable content.

Your Input
Any activity that could be deemed as ‘censorship’ has been demonstrated over the years to be a very controversial issue. As the population becomes more risk-aware, we expect over the long term to be using additional mechanisms (e.g. audit logs of use within institutions) in conjunction with varying levels of filtering.

As the Internet is firmly established as a global medium for business, education and entertainment medium, its value is likely to increase perpetually over the years. We suspect the issue of filtering will be with society in general for the foreseeable future, and so we all need to develop our strategies and ideas together.

As this is such a difficult area we depend very heavily on user feedback to choose the right course of action and welcome comments on this policy at any time via our email address: filtering@swgfl.org.uk

How to report inappropriate web sites
Please note that we maintain the right to ultimately determine what is and is not filtered. However, any of our customers who find a site that they feel should be filtered or unfiltered are asked to email filtering@swgfl.org.uk with the URL. We will review your requests against our filtering policy and notify you on the decision to permit or deny that site.

Further information and advice
Becta: http://schools.becta.org.uk/
Internet Watch Foundation: http://www.iwf.org.uk/
Filter Category Definitions

C.1 IWF Child Abuse Images database
Defined as content which the Internet Watch Foundation has identified as breaching UK law including: This list cannot be disabled.

C.2 Pornography and illegal or age-restricted activity
Defined as material containing sexually explicit images and text, the depiction of actual or realistic sexual activity or illegal or age-restricted activity including but not limited to:
  a real or simulated sexual intercourse including explicit cartoons/animation;
  b depiction of sexual activity involving devices such as sex toys;
  c sexual activity with visible pubic areas and/or genitals;
  d threats of sexual violence such as rape;
  e child abuse/paedophilia, excluding content classed as illegal by the IWF encompassed by C.1;
  f excessive use of profanity and/or obscene gesticulation;
  g erotic stories and textual descriptions of sexual acts;
  h sexually exploitative or sexually violent text;
  i content relating to cracked software application distribution;
  j content relating to pirated software and multimedia downloads;
  k content promoting, instructing, and distributing malicious executable software, viruses, worms, etc.;
  l other illegal or age restrictive activities, excluding the use of alcohol by minors encompassed by C.4.

NOTE Material which genuinely seeks to inform and educate such as content relating to current affairs, news, and historical information may be permissible.

C.3 Drugs and substance abuse
Defined as material relating to the use and promotion of illegal drugs, including but not limited to:
  a content promoting, encouraging or instructing on the use of illegal drugs, including the use of tobacco, alcohol and other substances illegal to minors;
  b information relating to the masking of drug use, including alcohol and tobacco;
  c content promoting the sale and distribution of illegal drugs;
  d information relating to recipes, manufacturing and growing of illicit substances;
  e content promoting and instructing on the use of illegal highs and the abuse of other legal substances;
  f content promoting and instructing on abuse of prescription drugs.

NOTE Material which genuinely seeks to inform and educate such as content relating to current affairs, news, and historical information may be permissible.

C.4 Violence (including weapons and bombs)
Defined as material containing graphically violent images and text, including but not limited to the following:
  a portrayal of graphic violence against humans, animals or institutions;
  b depictions of torture, mutilation, gore or horrific death;
  c content advocating self-endangerment, self-mutilation and suicide, including promotion eating disorders or addictions;
  d graphic violence that in particular dwells on the infliction of pain or injury;
  e instructions for making bombs and weapons;
  f portrayal and glamorization of easily accessible weapons, e.g. knives;
  g content promoting terrorism and terrorist organizations;
  h content promoting the use and purchase of weapons, ammunition, explosives, poisons, etc.

NOTE Material which genuinely seeks to inform and educate such as content relating to current affairs, news, and historical information may be permissible.

C.5 Intolerance
Defined as material which promotes intolerance, violence or attack on individuals or institutions on the basis of religious, racial or gender grounds, including but not limited to:
  a content that advocates or incites violence or attack based on religious, racial, ethnic, gender, age, disability, sexual orientation, or cultural community grounds;
  b content that advocates social intolerance;
  c promotion of political agendas based on supremacist, exclusionary, racial, religious, ethnic, gender, age, disability or sexual orientation grounds;
  d Holocaust denial, revisionist content and other sites encouraging hate;
Infrastructure Services

C.6  Web-based chat
Defined as unmoderated and unsupervised Web-based interactive chat or instant messaging that allows users to make contact with individuals in the outside world without paying sufficient attention to safeguards and protection for young people, including but not limited to:
   a  web-based interactive chat;
   b  web-based instant messaging.

C.7  Web-based social networking *New category*
Defined as unmoderated and unsupervised social networking that allows users to make contact with individuals in the outside world without paying sufficient attention to safeguards and protection for young people, including:
   a  web-based social networking that allows users to create a personal page or profile and construct and display a social network of their online contacts and/or supply personal information online in an unmoderated and unsupervised way.

C.8  Proxy bypass *New category*
Defined as material related to the creation and distribution of content related to Internet filtering circumvention including but not limited to:
   a  content promoting the unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network;
   b  content providing information relating to filtering applications and associated workarounds.

A.1  Web-based mail services
Defined as material that allows access to free web-based email services that can prove disruptive and distracting if used within an education environment, including:
   a  provision of free web-based email services.

A.2  Mobile phones, SMS and ring tones
Defined as material which promotes mobile phone manufacturers or their services and material which provides Internet based SMS services that can prove disruptive and distracting if used within an education environment, including:
   a  promotion of mobile phone manufacturers or service operators;
   b  promotion of free or chargeable mobile services;
   c  provision of Internet based SMS services;
   d  sites offering ring tones or downloadable phone icons.

A.2 .MP3 and .exe files
Defined as material that allows access to .MP3 files and .exe files used regularly by children for non-educational purposes, including:
   a  .MP3 files that can prove disruptive and distracting if used within an education environment;
   b  .exe files that can prove disruptive and distracting if used within an education environment.

A.3  Non-educational games *New category*
Defined as games that are not specifically designed to support content considered core to UK education curricula, including but not limited to:
   a  content relating to video, adventure, simulation, strategy and war games;
   b  content relating to board games, card games and puzzles.

Non-educational games that relate to pornography, illegal or age-restricted activities are included in the ‘Pornography and illegal or age-restricted activities’ category, rather than the non-educational games category.

Non-educational games that are violent are included in the ‘Violence’ category, rather than the non-educational games category.

NOTE Material which genuinely seeks to inform and educate such as content relating to current affairs, news, and historical information may be permissible.
## Category availability matrix

The matrix provided below outlines which categories are available for RM SafetyNet, and which are available for RM SafetyNet Plus and RM SafetyNet Universal.

<table>
<thead>
<tr>
<th>Core categories</th>
<th>RM SafetyNet</th>
<th>RM SafetyNet Plus and RM SafetyNet Universal</th>
</tr>
</thead>
<tbody>
<tr>
<td>IWF Child Abuse Images database</td>
<td>This list is always enabled</td>
<td>This list is always enabled</td>
</tr>
<tr>
<td>Pornography and illegal or age-restricted activity</td>
<td>This list is always enabled</td>
<td>This list can be amended locally in line with local Acceptable Use Policy</td>
</tr>
<tr>
<td>Drugs and substance abuse</td>
<td>This list is always enabled</td>
<td>This list can be amended locally in line with local Acceptable Use Policy</td>
</tr>
<tr>
<td>Violence</td>
<td>This list is always enabled</td>
<td>This list can be amended locally in line with local Acceptable Use Policy</td>
</tr>
<tr>
<td>Intolerance</td>
<td>This list is always enabled</td>
<td>This list can be amended locally in line with local Acceptable Use Policy</td>
</tr>
<tr>
<td>Web-based chat</td>
<td>This list is always enabled</td>
<td>This list can be amended locally in line with local Acceptable Use Policy</td>
</tr>
<tr>
<td>Web-based Social Networking</td>
<td>This list is always enabled</td>
<td>This list can be amended locally in line with local Acceptable Use Policy</td>
</tr>
<tr>
<td>Proxy Bypass</td>
<td>This list is always enabled</td>
<td>This list can be amended locally in line with local Acceptable Use Policy</td>
</tr>
<tr>
<td>Web-based mail services</td>
<td>This list is not available with RM SafetyNet</td>
<td>This list can be amended locally in line with local Acceptable Use Policy</td>
</tr>
<tr>
<td>Mobile Phones/SMS/Ring Tones</td>
<td>This list is not available with RM SafetyNet</td>
<td>This list can be amended locally in line with local Acceptable Use Policy</td>
</tr>
<tr>
<td>.MP3 and .exe files</td>
<td>This list is not available with RM SafetyNet</td>
<td>This list can be amended locally in line with local Acceptable Use Policy</td>
</tr>
<tr>
<td>Non-educational games</td>
<td>This list is not available with RM SafetyNet</td>
<td>This list can be amended locally in line with local Acceptable Use Policy</td>
</tr>
</tbody>
</table>

Categories should always be managed in line with the local Acceptable Use Policy.

Please note that if an education establishment with RM SafetyNet Plus or RM SafetyNet Universal cannot see these filter lists or the administration interface this is likely to be because the filter lists for that establishment are managed centrally by the Local Authority, RBC or other designated filtering administrator.
The security policy applied to the South West Grid for Learning (SWGfL) covers the following areas and protocols:

- Schools will be able to access Web sites on the Internet through Proxy Servers sited in the Core. Direct access to Internet Web sites from stations inside the SWGfL is not allowed.
- Schools will be able to have access to the standard RM news services. Access to other news services on the Internet is denied.
- The stations on the school’s LAN will be able to talk to DNS servers in the Core. This will allow DNS name resolution for all sites inside the SWGfL and the Internet.
- Stations and servers on the Internet will be able to browse to Web sites hosted on the Virtual Web Servers (VWS) sited in the Core. Schools within the SWGfL will be able to upload Web sites to the VWS.
- Video conferencing using the H323 protocol is only enabled through the SWGfL Gatekeeper. Sites can configure their settings on the Gatekeeper to control sites (internal and external) to which they can video conference. Also, importantly, schools that choose to have a local firewall or proxy may not be able to utilise the video conferencing service or may be limited to one designated video conference enabled station inside the LAN.
- SMTP Mail Relay Servers at the Core will handle mail between the Internet and the SMTP mail servers on the schools' LANs inside the SWGfL.
- If required schools can synchronise their computer's time with a designated time server at the Core.
- Management and backup of the Core servers are permitted from designated management stations at IFL (Internet For Learning).
- RM SafetyNet updates are allowed from the RM SafetyNet server to the Core sited SafetyNet Proxy Servers.
- All other traffic between establishments inside or outside the Grid will be blocked.

The table overleaf outlines the technical configuration of the central firewall service.

**Security Configuration**

The general principles of this security policy are as follows:

- No traffic shall enter or leave the SWGfL Infrastructure without being explicitly permitted by the firewall.
- No traffic shall route directly between connected establishments unless having been explicitly allowed to do so.
<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol/Port</th>
<th>Action</th>
<th>Log</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Establishments</td>
<td>WAN Centre Proxy/DNS Servers/VWS</td>
<td>HTTP8080 / DNS / FTP</td>
<td>Allow</td>
<td>No log</td>
<td>DNS Lookup</td>
</tr>
<tr>
<td>WAN centre child proxies</td>
<td>Virus scan proxies</td>
<td>HTTP</td>
<td>Allow</td>
<td>No log</td>
<td>Referral to parent proxy</td>
</tr>
<tr>
<td>Virus scan proxies</td>
<td>Internet</td>
<td>HTTP</td>
<td>Allow</td>
<td>No log</td>
<td>'Dirty' HTTP requests</td>
</tr>
<tr>
<td>WAN Centre Proxy/DNS Servers</td>
<td>The Internet</td>
<td>HTTP / HTTPS FTP / DNS</td>
<td>Allow</td>
<td>No log</td>
<td>Outbound proxy access to the Internet</td>
</tr>
<tr>
<td>Connected Establishments</td>
<td>WAN Centre News proxy</td>
<td>NNTP</td>
<td>Allow</td>
<td>No log</td>
<td>News (virus scan proxies as news proxies)</td>
</tr>
<tr>
<td>RM News server</td>
<td>WAN Centre News proxy</td>
<td>NNTP</td>
<td>Disallow</td>
<td>No log</td>
<td>News feed. WAN Centre news server acting as news proxy. Only allowed on explicit request.</td>
</tr>
<tr>
<td>Internet</td>
<td>WAN Centre VWS/DNS</td>
<td>HTTP / DNS</td>
<td>Allow</td>
<td>No log</td>
<td>Inbound HTTP for VWS</td>
</tr>
<tr>
<td>Connected Establishments</td>
<td>Internet</td>
<td>(H323)</td>
<td>Disallow</td>
<td>No log</td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td>Connected Establishments</td>
<td>(H323)</td>
<td>Disallow</td>
<td>No log</td>
<td></td>
</tr>
<tr>
<td>VC stations at sites (no Local firewall)</td>
<td>VC stations at sites (no local firewall)</td>
<td>(H323)</td>
<td>Allow</td>
<td>No log</td>
<td></td>
</tr>
<tr>
<td>Connected Establishments</td>
<td>VC stations at sites (with a local firewall)</td>
<td>(H323)</td>
<td>Allow</td>
<td>No log</td>
<td>Restricted to one identified station at the site with the local firewall</td>
</tr>
<tr>
<td>VC stations at Connected Establishments (with a local firewall)</td>
<td>Connected Establishments</td>
<td>(H323)</td>
<td>Allow</td>
<td>No log</td>
<td>Restricted to one identified station at the site with the local firewall</td>
</tr>
<tr>
<td>Connected Establishments</td>
<td>SWGfL SMTP Mail Relay Servers</td>
<td>SMTP</td>
<td>Allow</td>
<td>No log</td>
<td>Outbound SMTP</td>
</tr>
<tr>
<td>Any Host</td>
<td>SWGfL SMTP Mail Relay Servers</td>
<td>SMTP</td>
<td>Allow</td>
<td>No log</td>
<td>Inbound SMTP</td>
</tr>
<tr>
<td>Connected Establishments</td>
<td>SWGfL Mail Servers</td>
<td>POP3</td>
<td>Allow</td>
<td>No log</td>
<td>Inbound POP3</td>
</tr>
<tr>
<td>Connected Establishments</td>
<td>WAN Centre time server</td>
<td>NTP</td>
<td>Allow</td>
<td>No log</td>
<td>Time service to Connected Establishments</td>
</tr>
<tr>
<td>194.238.49.0/24</td>
<td>All WAN Centre equipment except fw-1 and fwmng</td>
<td>telnet / pcAnywhere pcAnywhere data pcAnywhere stat</td>
<td>Allow</td>
<td>short</td>
<td>IFL management connections to WAN Centre</td>
</tr>
<tr>
<td>Each WAN Centre subnet (not including .32/27)</td>
<td>Backup</td>
<td>Legato Ports</td>
<td>Allow</td>
<td>short</td>
<td>Rules to allow backup between subnets in WAN Centre</td>
</tr>
<tr>
<td>RM SafetyNet update server</td>
<td>WAN Centre Proxy Servers</td>
<td>331 SQL database update</td>
<td>Allow</td>
<td>No log</td>
<td>SafetyNet Updates</td>
</tr>
</tbody>
</table>

*Rules to allow any required connections to the Firewall from the FireWall Management Server*

*Rules to allow any required connections to the FireWall Management Server, such as management traffic from RM*

*Drop everything else trying to connect to the Firewall (stealth rule) & log*
Filtering Services in the SWGfL

Service overview
RM SafetyNet Plus is provided to assist you in implementing your Acceptable Usage Policies. By default a comprehensive level of Internet filtering is applied. However, RM SafetyNet Plus is a customisable solution, which allows you to create your own establishment’s filter list and tailor it to meet your needs.

RM SafetyNet Plus gives you complete control over which Web sites, Web searches and file extensions can be accessed within an establishment. Filtering rules may be added or overridden using the filtering administration interface. You could for example, create a walled garden - this restricts access to only the sites you select.

In addition to the default filter lists, RM SafetyNet Plus provides you with additional filter lists. For example, many establishments have implemented the Web-based email filter lists. This allows you to ensure users use SWGfL Mail, which you can monitor.

Your service entitlement
RM SafetyNet Plus is part of the core service. By default RM SafetyNet Plus filters sites in the following categories:

- Internet Watch Foundation Illegal Images database
- Pornography
- Drugs/substance abuse
- Intolerance
- Violence
- Web-based chat

It is strongly recommended that you do not turn off these categories.

The following filter lists are off as default, but may be turned on using the administration interface:

- Web-based email
- Mobile phones/SMS/ring tones filter list
- MP3 music files (*.mp3)
- Executable files (*.exe)

In addition to the provided filter lists you can use RM SafetyNet Plus to build your own filtering list. You can also build a list of banned searches.

All filtering settings in RM SafetyNet Plus will apply to your whole establishment. If you would like more refined filtering, for example the ability to filter by user/group/room, you may like to consider RM SafetyNet Universal for the SWGfL Content Delivery and Caching System.
Top three features/benefits of the SWGfL filtering service

1  Content filtering – technology which scans Web pages for key words and combinations of words, before deciding if the page should be filtered. This means that pages which have not yet been added to a list of banned Web sites, perhaps because the site has recently been published, may still be filtered.

2  Complete control – establishments are in complete control of their own filtering. This allows you to practically implement your establishment’s Acceptable Usage policies.

3  Additional optional filtering lists – such as the mobile Phones/SMS/ring tones filter list or the Web-based email list, help to keep pupils focused.

Getting you up and running with your SWGfL filtering service

How to log in to the SWGfL Filtering Administration Web site:

1  Browse to http://admin.filtering.swgfl.org.uk
2  Enter your Administrator username
3  Enter your password
4  Click the ‘Login’ button

FAQ - “I’ve forgotten my SWGfL filtering admin password.”

The administration of the filtering lists is a secure process; therefore the only way of resetting your password is to contact the SWGfL Managed Service team. They will need to see the request in writing (on your establishment’s letter-headed paper) before they go ahead.

How to set up a deny rule

A deny rule is a filter you can add to deny, block or ban a specific URL or type of Web site. An example of adding a URL that you consider to be distracting your pupils is given here:

1  In the rule box, make sure that you select ‘deny’
2  Click in the URL box and type in the Web site address
3  Click in the comment box and add something that will remind you why you’ve blocked this site
4  Click on the ‘Add URL’ button. This rule will then be added to the list
How to set up a permit rule

A permit rule is a filter you can add which permits, allows or authorises the viewing of a specific URL or type of Web site, which would otherwise be blocked by one of the filtering lists. Follow the same process as for adding a ‘deny’ rule, but choose ‘permit’ rather than ‘deny’ in the rule box.

How do the filtering lists work?

The filtering list you create at your establishment has the highest priority, i.e., it overrides those created at the LA or at the SWGfL level. This hierarchy of filtering lists is shown in the diagram below.

Content filtering is the scanning of HTML for banned words.

What is the unfiltered proxy?

Staff and pupils often have differing requirements from filtering. SWGfL filtering has an option called the ‘unfiltered proxy’ which can be used by staff to get unfiltered access to the Internet for administration use, while at the same time maintaining the pupils’ filtered lists. Clearly there are dangers attached to this feature and its use should be restricted accordingly.

Troubleshooting filtering

“Why can we browse to inappropriate sites?”

It is important to check that you have not included any ‘dangerous’ permit rules in your filtering site. Examples of these are:

Permit *.* - This is an inappropriate use of wildcards and has the effect of allowing everything.

Permit *.dk – In this case, all sites that originate in Denmark (domain.dk) are allowed to be viewed.
Remember – not a 100% Guarantee

No Internet filtering service can guarantee to prevent 100% of inappropriate sites from being viewed.

Should you find a Web site that has got through the filter but you believe should be blocked throughout the SWGfL, please take the following action:

1. Block the URL (Web address) using a deny rule as described previously. This will block access from your establishment to that URL immediately.

2. Send the URL in an email to the SWGfL Managed Service team at: urlfiltering@rmplc.co.uk so it can be added to the global filtering lists.

Please note that RM will only add sites to the RM SafetyNet global filter lists if they contravene RM’s or SWGfL’s filtering policy. To view the SWGfL filtering policy, please see the Safety and Security section, or visit the SWGfL Web site.

Hints and Tips

Tip – Always add a comment when adding a filtering rule

Once you have many rules in place, this will help you establish why something was originally blocked or allowed.

Tip – Customise the filter page

You can decide what is shown on the page that is displayed when a site is blocked (the ‘filter page’). This example shows how the page might look:
Service overview
We have improved SWGfL Filtering to support the Acceptable Usage Policy as detailed in ‘SWGfL Safe’.

The improvements provide:
• Auditing of attempted inappropriate access
• Audited use of the open proxy
• Easy visibility of recent changes to your filtering
• Monitoring of changes to Internet filtering settings
• Monitoring of Internet access not restricted by SWGfL Filtering
• Improved tools to support the filtering administrator’s role
• Internet Watch Foundation membership; browse to http://www.iwf.org.uk to read more
• Filtering that is accredited by Becta and supports the SWGfL Safety and Security policy

The improvements have been designed to:
• Improve the functionality of the SWGfL Filtering system to reduce inappropriate use of an establishment’s Internet services
• Prevent accidental or deliberate access to inappropriate material
• Increase security for system administrators and, with their knowledge, all activities are monitored for review by the school’s senior management team

Your service entitlement
The SWGfL Filtering improvements will be deployed to all establishments.

Top three features / benefits of the filtering improvements
1 Audited use of the Open Proxy – where staff require a greater level of access to the Internet, a username and password can be provided. All access will be fully audited for the user’s protection. Audit trails are available for school management teams to review

2 Logs of administration changes – all changes to the filtering settings are logged along with the time, date, IP address, and user ID, for the protection and support of the administrator

3 Tools to make administration easier – to help with housekeeping, if your filter rules are subsequently included in the core list, you will be notified so that you can remove this duplication
Notification of filter list additions

SWGfL filtering is powered by RM SafetyNet Plus, one of three products in the RM SafetyNet range. RM SafetyNet is used by more UK education establishments than any other solution. The specialised range is proven, trusted and widely adopted by education establishments, from primary schools to universities.

It provides the ability to customise filtering by establishment or region and utilises a combination of sophisticated methods which work together to provide highly-effective web-filtering for education.

SWGfL Filtering now includes new optional filter lists for proxy bypass sites, non-educational games and social networking.

These new, additional, filter lists are available to SWGfL Filtering customers free-of-charge.

More information on these new categories, and the action that you need to take, is provided in this document.

Enhanced proxy bypass detection

Proxy bypass sites, originally created to circumvent internet censorship in China, constantly evolve as their developers find new ways to side-step content filters.

Typically, a proxy bypass site would allow a user to enter a web address that is normally filtered, such as http://www.unsuitablesite.com, and then submit a request to download this web page and subsequently pass the unsuitable web page on to the user. The request might look something like:


SWGfL Filtering already blocks such requests. More recently, proxy sites have started to avoid this type of filtering by encoding the URL being passed within.

Some types of encoding include Base 64 encoding, Rot13 encoding and Q-tunnel encoding. This request might look like:

http://www.qtunnel.com/index.php/1010110A/1e70c93886b92f7920f6f9f149f86e7022060

Decoding these strings can create a negative effect on Internet and filtering speed. The SWGfL Filtering Enhancement has negated this limitation by developing a new detection engine which can identify these proxy bypass sites automatically and subsequently block them, without a negative impact on performance! This combines URL within URL filtering with advanced pattern-recognition technology to detect and block ciphered URLs. Proxy bypass detection is significantly improved by this thorough, automated approach.

A new filter list has been created to categorise these proxy bypass sites. This will be visible on your administration site. We advise that this list is always enabled.

Tip – Your tasks

This enhancement has been implemented remotely; there is no need for you to download new software. Your personalised filter settings will not be deleted but you will need to review your own filter lists to exploit most from these new enhancements.
Social networking filter list

Social Networking sites are blocked by SWGfL filtering as standard due to the potential risks that they can pose for children and young adults as well as the distraction they may cause. We have now created a separate filter list for Social Networking sites to enable administrators to unblock these sites should they contravene a local (school) Acceptable Use Policy.

Establishments most likely to allow access to these sites may be Secondary schools, in contrast to those with younger students.

The new social networking filter list is optional; the filtering administrator has the ability to turn this list off should the establishment or region’s Acceptable Use Policy not require it.

Non-educational games filter list

Violent and pornographic games are already blocked as standard by SWGfL Filtering. Release of a new non-educational games filter list will enable blocking of nonviolent and non-pornographic games which are used regularly by children for non-educational purposes.

The new non-educational games filter list is optional; the filtering administrator has the ability to turn this list on should the establishment or region have a policy to do so.

The SWGfL Filtering Policy is available at: [www.swgfl.org.uk/services/refpack/safety_and_security/internetaup.pdf](http://www.swgfl.org.uk/services/refpack/safety_and_security/internetaup.pdf). Please refer to this and to your local filtering policy to determine whether these lists should be enabled or disabled for your establishment or region.

Release dates

This evolution of SWGfL Filtering was enabled in July 2008.

Words of caution

Care should always be taken when changing filtering levels. For example, access to social networking sites in structured programmes can be immensely useful to help support the education of children to help themselves to be safer online both in and out of school.

By unselecting filter lists, staff should be aware of other users usage and whether this access is having any other effect across the organisation or school. In this example, it may be preferable to not deselect the social networking filter list but to permit access to the specific social networking site required as part of the education programme. Using the SWGfL Monitoring tool will help to monitor this site-based usage.

The new lists will be enabled or disabled as standard at point-of-upgrade as follows:

- **Proxy Bypass filter list** - selected as standard, administrators can disable this list if it is not required
- **Social Networking filter list** - selected as standard, administrators can disable this list if it is required
- **Non-Educational Games filter list** - unselected as standard, administrators can enable this list if it is required

Filter lists can be enabled or disabled by your filtering administrator by checking or unchecking the associated box on the web-based administration interface. Please review your filtering settings when we release these new lists, and change your local settings if required.
Filtering Developments

At the end of 2006 various changes were made to how SWGfL Filtering is administered in the SWGfL. The most important parts of this have been the introduction of:

1. **Staff Proxy** - This will provide audited access (via individual user name and password) to all Web sites except those categorised as illegal by the Internet Watch Foundation. i.e. the staff proxy allows access to web sites which would normally be filtered by an establishments filtering policy.

2. **Update Proxy** – This provides the ability to download software updates (e.g. Virus updates) under the protection of an establishments filtering configuration.

3. **Read Only Users** - It is possible to provide Read Only permissions to users. You might for example choose to provide this to members of the Senior Management Team.

To help SWGfL sites move away from the unfiltered proxy, we have put together this document to give you tips on how to use the Staff and Update proxies. In addition, full details of how to use them are available from: [http://www.swgfl.org.uk](http://www.swgfl.org.uk)

**Why we’ve made these developments**

In line with the concept of ‘SWGfL Safe’, these developments will reduce the risks associated with Internet use in an educational environment. They will provide the evidence that may be required to demonstrate that filtering is being managed correctly at every site, while encourage administrators to act appropriately as their actions are being monitored and an audit trail of changes is being created.

**What this means for the Unfiltered Proxy**

The SWGfL is committed to monitoring and auditing the use of the internet to see whether users are complying with the acceptable usage policy. A key step to this will be to migrate all users of the unfiltered proxy over to the staff and update proxies.
Staff Proxy Tip 1: Creating Users
1. Log into the SWGfL Filtering Administration Web site – http://admin.filtering.swgfl.org.uk
2. Choose Settings > User Management
3. Select Add, and complete the form with the details of the new user.
4. Next to Permissions, tick the box marked Staff Proxy
5. Click OK, and a new user will be created.

Staff Proxy Tip 2: Allowing Use
1. Log into the SWGfL Filtering Administration Web site – http://admin.filtering.swgfl.org.uk
2. Choose Settings > Local Admin Details
3. Select Allow use of Staff Proxy and enter a date that access to the Staff Proxy will expire
4. Click to save changes

Staff Proxy Tip 3: Logging on to the Staff
1. Type ‘login.staffproxy’ in the address bar of your browser
2. When prompted, enter your user name and password, click OK.
3. Read and Accept the Acceptable Usage Policy Staff Proxy access will now be available until the Web browser is closed.

Staff Proxy Tip 4: Using the Staff Proxy with Internet Explorer
1. Open Internet Explorer and go into LAN settings, and tick ‘Use Proxy Server for your LAN’
2. Enter ‘staffproxy.swgfl.org.uk’ in the address box and specify port 8080, and Click OK
SWGfL Filtering: Update Proxy

The Update Proxy allows users to access sites which contain software updates such as virus dates or the Windows Update whilst still protecting users with the establishments filtering policy.

Update Proxy Tip 1: Using the Update Proxy with Internet Explorer

1. Open Internet Explorer and go into LAN settings, and tick ‘Use Proxy Server for your LAN’
2. Enter ‘updateproxy.swgfl.org.uk’ in the address box.
3. Click OK
SWGfL Filtering: Read Only Users

One of the five outcomes of the Every Child Matters agenda is Staying Safe. This provides a mechanism for members of the Senior Management Teams to check filtering settings and ensure they are safe and appropriate.

Read Only Tips: How to create a read only user

1. Log into SWGfL Filtering > http://admin.filtering.swgfl.org.uk
2. Choose Settings > User Management from the menu > Select Add
3. Complete the form with the detail of the user
4. Next to Permissions tick the box marked View Filtering Rules > Click OK

A user will now be created with the username in the format of username.establishmentID

A read only user may log into filtering in the usual way, and they will be able to view the filtering configuration, but not make any changes.

SWGfL Managed Service Team

Support for the SWGfL can be obtained any time within the hours 8.00am and 6.00pm, Monday to Friday (excluding Bank Holidays).

Contact can be made via the following means:

Telephone: 0845 3077870
Fax: 01235 826893
Email: support@swgfl.org.uk
Dealing with Proxy Bypass Web Sites

What is a Proxy Bypass web site?

Proxy bypass sites are websites on the Internet that enable users to get around filtering systems by simply visiting their website and typing in any URL (such as www.myspace.com). This will cause all connections and traffic to and from the URL to be redirected via the proxy bypass site. This tricks the SWGfL web proxies into believing that the web requests are coming from the proxy itself, thus circumventing SWGfL Filtering. So, by using a bypass proxy, users can access any website that would normally be filtered.

These websites have been used to bypass the censorship that exists for the Internet within China. Most of these web based proxy bypass sites are free and the list of such sites is growing all the time as more and more people try to satisfy the growing need for such services to bypass the network restricted access to various sites.

Once identified, SWGfL filters “Bypass Proxy” sites as it contravenes the responsible use of SWGfL as outlined in the SWGfL Acceptable Usage Policy.

Are children using these web sites in the SWGfL?

The SWGfL is committed to monitoring and auditing use of the internet to see whether users are complying with the acceptable usage policy. Unfortunately we have recently identified an increasing number of web requests being made to “Proxy Bypass” web sites. This means that pupils and staff in the SWGfL have been gaining access to web sites that would usually be filtered by SWGfL Filtering. We know that social networking sites such as Facebook, MySpace and Bebo have been accessed by pupils using these “Proxy Bypass” web sites.

The potential dangers associated with pupils circumventing SWGfL Filtering and accessing the sites such as those above are very significant. Becta (E-safety 2005) identifies the following risks:

- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Cyber bullying, physical danger and sexual abuse

The number and frequency of requests to proxy bypass web sites from with the SWGfL has reached a level where we feel it’s important to raise the awareness of these sites, what the SWGfL is doing to prevent their use, and what schools can do.
What are the SWGfL doing to reduce the risks that “Proxy Bypass” sites pose?

In response to the increasing problem of “Proxy Bypass” sites we have developed a new automated tool that performs two functions:

- Firstly, it proactively scans the Internet looking for “Proxy Bypass” sites. Using known “Proxy Bypass” sites, the tool follows each linked site and checks to see if it is a “Proxy Bypass” site. This is very similar to the way that internet search engines identify and index websites.

- Secondly, it automatically reviews the most popular 100 sites with each Local Authority in the SWGfL identifying “Proxy Bypass” sites that have been accessed.

What can you do to help reduce the risks that “Proxy Bypass” sites pose?

Firstly, if you find a “Proxy Bypass” site that is not filtered, add it to your schools filtering list, in addition please submit it to filtering@swgfl.org.uk for addition to the central filter list to help other schools.

Secondly, make sure that all your users are aware of the school and SWGfL AUP. The purpose of the SWGfL AUP is to ensure that users understand the way in which the Internet is to be used. The policy aims to ensure that the Internet is used effectively for its intended purpose, without creating unnecessary risk.

Thirdly, encourage good Internet use, by making all users aware of the risk of using such sites.

Finally, use the SWGfL Monitoring site to review the information for your school in SWGfL Monitoring. This offers you a wide range of information, about the use of your schools connection. Using the top 100 most requested web sites, you will be able to review if there is a significant issue of users making use of “Proxy Bypass” web sites.

SWGfL Monitoring site can be accessed by browsing to http://monitoring.swgfl.org.uk
EDUCATION AND RESOURCES

SWGfL E-Safety Day
Education Programmes for KS1
Education Programmes for KS2
Education Programmes for KS3
Education Programmes for KS4
E-Safety for Parents and Carers
Web Exploration Session
Teaching E-Safety
South West Grid for Learning - SWGfL E-SAFETY DAY

Is your school community aware of online technologies and the risks?

Educating your children, staff, governors and parents

Taking and tailoring recognised e-safety programmes and resources, SWGfL is able to provide e safety experts to deliver targeted education sessions across an extended school day to your children, staff, governors and parents.

A bespoke E Safety day can be tailored delivering components such as:

1 Assembly – The day could start with an interactive assembly, stimulating interest and discussion

2 Children – Taking groups of children to receive recognised and relevant e-safety programmes in hour long workshops. Example programmes cover KS1 to KS4 and include:
   - KS2 – CEOP’s Cybercafe
   - KS3 - CEOP’s Think u know

3 Staff – Introducing staff to web 2.0 technologies and their use and misuse. The session will offer strategies for managing risks and issues as well as where they should get help. Staff will be left with resources such as Childnet’s Know it all for teachers

4 Governors – Governors carry an equal responsibility to ensure the safety of children, this session will, through outlining technologies and strategies, stimulate conversation, support and engagement

5 Parents – Culminating with a parents evening, parents will be introduced to the online environments their children are using and provide them with what to look out for and strategies for ‘what they can do’.

What a Primary school e-safety day might look like

<table>
<thead>
<tr>
<th>Time</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>9am</td>
<td>Assembly</td>
</tr>
<tr>
<td></td>
<td>KS1 Workshop</td>
</tr>
<tr>
<td></td>
<td>Lunch Awareness</td>
</tr>
<tr>
<td></td>
<td>KS2 Workshop</td>
</tr>
<tr>
<td>4pm</td>
<td>KS2 Workshop</td>
</tr>
<tr>
<td></td>
<td>INSET</td>
</tr>
<tr>
<td>7pm</td>
<td>Staff / Governors</td>
</tr>
<tr>
<td></td>
<td>Parents evening</td>
</tr>
</tbody>
</table>
SWGfL E-Safety Day: FAQ

Why do I need to look at E-Safety?
Many children embrace and exploit the power of the Internet and online technologies for many different aspects of their lives for significant benefit. This is often foreign and difficult for many adults to understand, leading to the increasing gulf between today’s digital natives and digital immigrants*. Although this technology has huge benefits, there are also associated risks, some of which children are not aware.

Ask yourself – who taught your children to use MSN? How do children know what the risks are? Schools and parents and wider society have an obligation to safeguard its children and the online environments are no different. In essence why Internet safety is due to be included in the KS3 curriculum from September 2008.

* Marc Prensky 2001

How will the day be organised?
The structure, aims and objectives of the day will be organised in advance and in conjunction with the school. This will enable the expert to tailor resources and programmes for each school.

Can I deliver these resources myself?
Yes. All the resources and programmes are available directly from SWGfL partners. SWGfL is aiming to help and support those schools who don’t feel able to deliver these messages themselves.

How will this enable my school to embed e-safety?
There are a number of objectives of the day that aim to embed e safety into the school.

1. Provide the school staff and parents with confidence and resources to support and carry on the education programme and awareness raising
2. Stimulate conversation across the different school communities
3. Engage governors and leaders to consider e safety policies, processes and provision

What is the cost?
POA

This includes the delivery of the tailored day and the resources left with the school.

Want to find out more?
Contact SWGfL at enquiries@swgfl.org.uk or phone 01392 381371
Are infants too young to learn about staying safe online?

Recent research from OFCOM (2008) showed that of 5 to 7 year olds:

- 59% access the internet at home
- and that 21% do so unsupervised

Access to the Internet and the opportunities it enables is ever increasing. As OFCOM found, this access is no different for infant age children and whilst their utilisation of mobile and online technologies is generally lower than their older peers, it is often significantly higher than you might imagine. It is vitally important that infant age children are helped to be able to navigate through the online world in a supportive and controlled manner in preparation of their use as they continue to grow and explore.

There are a number of emerging resources and programmes aimed at KS1 children to help them to stay safe when online; this document signposts a number of key examples.

**Staying Safe online – CEOP Thinkuknow Hector’s WorldTM**

Hector’s WorldTM comprises five state-of-the-art, animated episodes. It takes children on a journey with Hector and his friends as they explore issues such as personal information, trustworthiness, making positive choices online and how to be open with a trusted adult when they use the internet.

The animation has been adapted for a young UK audience following successful running of the programme in New Zealand and is backed up by a series of free resources.

Access to the Hector’s World, including lesson plans are available at: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

---

1 Ofcom’s submission to the Byron Review, Annex 5: The evidence base - the views of children, young people and parents’, 27th March 2008
Staying Safe contd. - NetSmartz Workshop

The NetSmartz Workshop is an interactive, educational safety resource from the National Center for Missing & Exploited Children® (NCMEC) and Boys & Girls Clubs of America (BGCA) for children aged 5 to 17, parents, guardians, educators, and law enforcement.

For the youngest children, NetSmartz have created special animated characters that help deliver targeted online and offline activities.

More information can be found at [www.netsmartz.org/resources/nsresources](http://www.netsmartz.org/resources/nsresources).

Activities – BBC Stay Safe

The BBC has created a series of cartoons and quizzes all presented by the character, Dongle. The site also includes printable factsheets specially aimed at KS1 children.

Further information can be found at: [www.bbc.co.uk/cbbc/help/safesurfing/](http://www.bbc.co.uk/cbbc/help/safesurfing/)

What about their parents?

Parents are often unaware of how their children use mobile and online technologies. Childnet International have produced Know it all for parents. The resource is available as a CD or online for schools to order from DCSF publications free of charge to provide to their parents (quoting 00308-2007CD-EN).

Does your school run parents evenings on Internet safety?

If you do not feel your school have the necessary experience or expertise to present this material, have you considered SWGfL e safety days? Please contact SWGfL for more information.
How does your school help educate its children as to the risk when online?

Recent research from OFCOM (2007) showed that of 8 to 11 year olds:
- 40% are now using the Internet
- 75% have their own mobile, television or games console offering online access

It is clear that adoption of mobile and online technologies are significantly increasing amongst the 8 to 11 year old age range. These technologies include Instant Messengers (such as MSN), Social networking sites (such as Bebo) and chat sites (such as Habbo Hotel) and whilst minimum ages are usually set at 13, many children engage at younger ages. Much of the use is self or peer taught with often little appreciation of the real risks. Historically online safety education has been focused on secondary age children but this change requires that this is now replicated across all primary age ranges and especially KS2.

This document outlines the programmes and strategies that are available for schools to educate KS2 children to help protect themselves and stay safe when online.

**Staying Safe online – CEOP Thinkuknow Cybercafé**

Created by CEOP (Child Exploitation and Online Protection Centre [www.ceop.gov.uk](http://www.ceop.gov.uk)) in partnership with Becta, DCSF and Gridclub, the cybercafé allows children to explore 9 online and mobile technologies in a safe activity based environment. Linked with each technology is an associated and detailed lesson plan.

The activities all provide advice tips alongside a simple Stop, Think and Go approach, ensuring that the key points are made.

Access to the Cybercafe and further details including lesson plans are available at: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
Staying Safe Online contd – Kidsmart

Kidsmart is an award winning practical site for children, teachers and parents, produced by Childnet International. The site has a special area for teachers, including an array of lesson plans all aimed at different areas of online technologies, how to have fun but critically staying safe. Accompanying the lesson plans are worksheets and teachers notes.

More information can be found at [http://www.kidsmart.org.uk](http://www.kidsmart.org.uk)

What about their parents?

Parents are often unaware of how their children use mobile and online technologies. Childnet International have produced Know it all for parents. The resource is available as a CD or online for schools to order from DCSF publications free of charge to provide to their parents (quoting 00308-2007CD-EN).

Does your school run parents evenings on Internet safety?

Cyberbullying – Digizen.org

Launched in September 2007 by Childnet International, the Digizen site includes full guidance on cyberbullying, what it is, as well as how to prevent it and how to respond to it. Accompanying the guidance is an excellent new resource including a full lesson plan. The lesson uses a film and associated interviews to make the necessary points. This is available both on the web and as a DVD.

Further information can be found at: [www.digizen.org](http://www.digizen.org)

If you do not feel your school have the necessary experience or expertise to present this material, have you considered SWGfL e safety days? Please contact SWGfL for more information.
Does your school educate its children to stay safe online?

ICT has long been an integral part of the curriculum, but ask yourself the question: “who taught your children to use instant messengers such as MSN?”

Today’s digital natives* use and exploit online and mobile technologies in all aspects of their lives, for education, entertainment, communication, expression, the limits are boundless. The continued evolution of these technologies, coupled with their near universal adoption, especially across the 11 to 16 age range, further extends the gulf between the digital natives* and digital immigrants*. In many cases, children and young people have engaged with these technologies within their own groups and communities and whilst the majority of use encourages and develops their growth and engagement, there is the potential for risk or misuse. Now is the time to engage with children and young people to help them to stay safe online, especially as it is a requirement of the Y7 curriculum from September 2008. There are many programmes that can stimulate and educate on Internet safety; this document highlights a number of such resources.

* Marc Prensky 2001

Staying Safe online – CEOP Think u know

Created by CEOP (Child Exploitation and Online Protection Centre www.ceop.gov.uk) and launched in July 2006, the excellent Think u know programme is aimed at KS3 children.

Lasting around 50 minutes, the structured programme is delivered by recognised trainers and covers how to fun, how to stay in control and how to report a problem. Using award winning films, the programme structure enables children and young people to understand the risks and issues and how they can protect themselves. In the first 12 months, over 1million children and young people benefited from the programme.

To become a recognised trainer or to arrange Think u know sessions to be run at your school by your local police or SWGfL, please contact SWGfL at the details below or visit: www.thinkuknow.co.uk
Staying Safe Online contd – Jenny’s Story

Jenny’s story, created by Childnet International, is a hard hitting film based on a true story about a young teenager who, after revealing personal information, was contacted in real life and ultimately hurt. The resource is supported by lesson plans and challenges children to think about their actions.

More information can be found at: http://www.childnet-int.org/jenny/

Childnet International

Childnet International has a series of excellent teaching resources including lesson plans such as Kidsmart and Blog Safety, all aimed at making the Internet a fun and safe place for children.

Further information can be found at www.childnet-int.org

Cyberbullying – Digizen.org

Launched in September 2007 by Childnet International, the Digizen site includes full guidance on cyberbullying, what it is, as well as how to prevent it and how to respond to it.

Accompanying the guidance is an excellent new resource including a full lesson plan. The lesson uses a film and associated interviews to make the necessary points. This is available both on the web and as a DVD

Further information can be found at: www.digizen.org

What about their parents?

Parents are often unaware of how their children use mobile and online technologies. Childnet International have produced Know it all for parents. The resource is available as a CD or online for schools to order from DCSF publications free of charge to provide to their parents (quoting 00308-2007CD-EN).

Does your school run parents evenings on Internet safety?

If you do not feel your school have the necessary experience or expertise to present this material, have you considered SWGfL e safety days? Please contact SWGfL for more information.
Web technologies are second nature to 14 – 16 year olds, how do you keep them safe?

Recent research from OFCOM (2008)1 showed that of 12 to 15 year olds:

- 55%1 have a profile on a social Networking website
- 90%2 have their own mobile phone
- Access the Internet for an average 13.82 hours per week at home

It is perhaps the 14 to 16 age range that makes most use of the amazing opportunities that the Internet and mobile technologies offers, as this research from OFCOM clearly demonstrates. As children develop and mature, it is still important to help safeguard them, and this age group is no different. At this stage, they will generally have a very high degree of technical competency, and in some cases this might not yet be matched by an equal ability to assess risk. At this stage a different approach is evidently required to help them stay safe when online.

The following represent relevant Internet safety resources and programmes targeted at 14 to 16 year olds.

**Staying Safe online – CEOP Thinkuknow ‘Matt thought he knew’**

The standalone lesson and DVD resource produced by CEOP as part of Thinkuknow, follows Matt as he makes friends online and the ensuing issues and situations he encounters. To supplement the film, there are a number of activities that stimulates discussion and outline both how to stay safe and also what action can be taken in such circumstances.

Accompanying resources and posters are also available from the Thinkuknow website. To order the DVD, lesson plan and resources, you are required to register at:

[www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

---

1 Social Networking; A quantitative and qualitative research report into attitudes, behaviours and use, OFCOM, 2nd April 2008
2 Media Literacy Audit, Report on UK children’s media literacy; OFCOM, 16th May 2008
Staying Safe contd – CEOP Think u know

Thinkuknow was CEOP’s (Child Exploitation and Online Protection Centre) first education programme and launched in July 2006. Created to last for 50 minutes, the lesson challenges children and young people to consider the risks associated the Internet, their own uses and how they might report any issue. Although primarily aimed at KS3, it has relevance for KS4.

CEOP require that anyone wishing to use this Thinkuknow resource is authorised having attended training.

More information can be found at: www.thinkuknow.co.uk

What about their parents?

Parents are often unaware of how their children use mobile and online technologies. Childnet International have produced Know it all for parents. The resource is available as a CD or online for schools to order from DCSF publications free of charge to provide to their parents (quoting 00308-2007CD-EN).

Does your school run parents evenings on Internet safety?

Childnet International

Childnet International have been pioneers in Internet safety education since 1996 and have developed an array of exceptional resources aimed at making the Internet a fun place for children and young people whilst helping them to stay safe. Here are examples of the resources available.

Further information can be found at: www.childnet-int.org

Examples

Cyberbullying film and lesson plan, ‘Let's Fight it Together. Hard hitting film and lesson plan based on a true story

Jenny's Story digizen.org

NetSmartz Workshop

The NetSmartz Workshop, from the National Centre for Missing and Exploited Children in the United States, has an array of Internet safety resources, including Real-Life Stories aimed at older teenagers. Each film has accompanying activities.

Further information can be found at: www.netsmartz.org/resources/reallife.htm

If you do not feel your school have the necessary experience or expertise to present this material, have you considered SWGfL e safety days? Please contact SWGfL for more information.
E-Safety for Parents and Carers

Parents either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”

Marc Prensky coined the phrase digital natives and digital immigrants in 2001 to represent the general polarised use of digital technology by children and young people (digital natives) and adults (digital immigrants). Parenting is a hard enough responsibility but with little or no knowledge of the new virtual worlds children populate, it is made almost impossible. Research highlights some of these gaps. Of adults:

• 67% of adults were not interested in Social Networking sites

• Only 13% of parents thought that they knew more about the Internet than their 12-15 year olds

• Lack of knowledge of how their children use the internet - 30% of parents thought that their children’s social networking profile was publically available compared to 41% of children who reported that their profile was actually publically available

As with real life there are risks and issues to be aware and wary of but it’s important to have a balanced approach and remember that online and mobile technologies open a world of opportunities to learn, explore and develop. It is important that parents recognise the digital divide and take action to engage their children in these new virtual worlds as they do in real life.

So what can be done? … What contribution can schools make?

Effective ways need to be found to stimulate and support parents to engage with their digitally capable children.

The Byron Review

In the Byron Review', Dr Tanya Byron recommended that schools “offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues”. The report also comments that e-safety messages “should be targeted towards grandparents and other relatives as well as parents.”

Continued over are practical resources you can use

1 Safer Children in a Digital World: the report of the Byron Review, 27th March 2008
2 Social Networking: A quantitative and qualitative research report into attitudes, behaviours and use, OFCOM, 2nd April 2008
3 Media Literacy Audit, Report on UK children’s media literacy; OFCOM, 16th May 2008
Resources – Know it all for Parents

Know it all for Parents was commissioned by DCSF and created by Childnet International in 2007. It is an amazingly comprehensive interactive resource that presents the issues in a clear and concise manner. It includes a wealth of strategies, tips and tools to help parents to understand and minimise the risks without detracting from the positive opportunities that the Internet enables.

The resource is available online or in CD format. Copies of the CD are currently free for schools to order and available from DCSF publications (quoting 00308-2007CD-EN).

More information can be found at: www.childnet.com/kia

E Safety Parent Evenings and the SWGfL Parent Programme

SWGfL has been delivering e safety sessions since 2006 at schools across the South West and in 2008, with the South West Police Forces, embarked on an ambitious aim to extend this programme to cover the whole region and therefore all parents, organising events within school clusters. The content includes an overview of the new online and mobile technologies alongside the actual risks and issues that aims to both support and stimulate parental engagement as well as providing practical strategies and tools to assist parents.

Further information and event locations can be found on the SWGfL website: www.swgfl.org.uk/safe

The GOLDen rules

SWGfL have developed the GOLDen rules that provide simple pointers to help safeguard parents and children whilst using the Internet.
SWGfL Web Exploration Session

Never accessed web 2.0 technologies such as Facebook or Bebo or find they are simply blocked?

Want to do this in a controlled environment?

SWGfL has designed half or one day sessions to allow you to explore and experience the array of web 2.0 technologies

Aimed at any professional working with children, the session aims to provide access to the web 2.0 technologies in a controlled and safe manner.

Children and Young people have significantly embraced the so called web 2.0 online and mobile technologies. These technologies exist in a world, often very foreign for many adults who have not grown up with them but are having to learn to adapt. This makes safeguarding or teaching children about the issues significantly harder as many professionals have either no or little personal experience (certainly compared to their audience).

The course aims to:

• Provide delegates with personal experience of web 2.0
• Through personal understanding, raise teacher confidence
• Provide an array of relevant and practical resources and programmes

The course will enable delegates to:

• Recall personal experience when helping children and young people
• Understand how some of the websites and online environments work and their purpose
• Experience how children and young people use web 2.0
• Consider how to safely access such environments in a professional capacity

The course will:

• Enable delegates to access sites and online environments such as Bebo, Facebook, Habbo Hotel, Second Life, Runescape
• Allow delegates to create and manage personal profiles
• Control the online environment
Why do I need to understand Web 2.0?

Credibility and confidence - In order to effectively communicate the issues and risks associated with the online and increasingly mobile environments, it is important to have a basic understanding in order to remain credible. To have a basic grasp of the array of technologies that children and young people use will significantly help the flow of any related safety session.

Equally the technologies can be powerful, inspiring uses not only within personal use but also in a working context.

How will the day be organised?

The majority of the session will set aside for delegates to explore the technologies although a number of structured exercises and suggestions will be provided. It is critical that delegates are free to explore the areas of these technologies that are relevant to their professional capacity.

How can I access these environments?

The filters are temporarily removed for the duration of the session to enable delegates to access and experience. Delegates should consider how they can access these areas post session.

How will this help my school?

There are a number of objectives of the day that will help school.

1. Provide delegates with confidence and personal experience to be better able to deliver e-safety sessions to not only students but also staff and the wider community.

2. Have staff that better understand these technologies to help support or manage any potential or actual safeguarding issues within the environments.

What is the cost?

£ POA

This includes the delivery of the tailored day and the resources left with the school.

Want to find out more?

Contact SWGfL at enquiries@swgfl.org.uk or phone 01392 381371
Do you feel suitably confident and equipped to teach about e-safety and manage the issues in the classroom?

A BT commissioned survey (2006) concluded 61% of UK teachers do not feel sufficiently trained to deal with the growing issue of child safety on the web.

To help to address this, SWGfL has designed this one day course for head teachers, teachers, teaching assistants.

Children and Young people have significantly embraced the so called web 2.0 online and mobile technologies. These technologies exist in a world, often very foreign for many adults who have not grown up with them but are having to learn to adapt. As children explore these technologies schools have a vital role to play in helping to safeguard them in these new worlds. This task is not easy, as the BT survey concluded, with many teachers not feeling sufficiently confident or trained to either manage or teach about e-safety.

The course aims to:

- Introduce delegates to the online and mobile technologies that children and young people use and the associated risks
- Through understanding raise teacher confidence
- Provide an array of relevant and practical resources and programmes

The course will enable delegates to:

- Put together a plan for teaching E-Safety throughout the school
- Raise awareness of E-Safety issues for parents
- Review the school’s policy for ensuring and teaching e-Safety in particular how schools can deal with e-Safety issues (cyber bullying, how to monitor web use, useful websites for teaching/supporting E-Safety);

The course will cover:

- The risks and benefits of using modern online and mobile communication technologies
- What can schools do to help – this section contains an overview of the best resources and time to actually try these out.
- How can we communicate some of these issues to parents?
- How can we communicate these issues to colleagues back at school?
- How do we ensure that our policies at school are up to date and include everything that we need in order to keep children and young people safe when using these technologies?
SWGfL Teaching E-Safety: FAQ

Why do I need to look at E-Safety?
The recently published Byron Report commissioned by the Prime Minister made several recommendations all of which have been accepted by the government. It said that “in good schools, all staff will have a role with regards to e safety” and goes on to recommend that “school leaders and teachers to focus on e-safety by identifying it as a national priority for continuous professional development (CPD) of teachers and the wider school workforce“. Further, it recommends that “Ofsted take steps to hold schools to account“.

In conclusion, the Byron report comments that; “to ignore e safety issues when implementing the Every Child Matters agenda would be a major oversight and would ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable.”

A copy of the Byron report can be accessed at [www.dfes.gov.uk/byronreview](http://www.dfes.gov.uk/byronreview)

How will the day be organised?
The day will comprise a mixture of practical sessions as well as the chance to hear about current developments around e-safety. There will be plenty of opportunities for participants to browse some of the resources and consider how they can use these back in school. An overview of filtering and monitoring will also be given.

How will this enable my school to embed e-safety?
There are a number of objectives of the day that aim to embed e-safety into the school.

1. Provide the school staff with confidence and resources to support and carry on the education programme and awareness raising with pupils, staff, parents and governors
2. Stimulate conversation across the different school communities
3. Engage governors and leaders to consider e safety policies, processes and provision

What is the cost?
£ POA

This includes the delivery of the tailored day and the resources left with the school.

Want to find out more?
Contact SWGfL at enquiries@swgfl.org.uk or phone 01392 381371