



M86 Response to Department for Children, Schools and Families (DCSF) Guidance on Cyberbullying

Developed by Childnet International

The guidance document, "Cyberbullying - Safe to Learn: Embedding Anti-bullying Work in Schools," (Guidance) was developed by Childnet International in consultation with the Department for Children, Schools and Families (DCSF) Cyberbullying Taskforce. Excerpts are reproduced under the terms of the Crown Copyright Click-Use Licence.

The Guidance provides:

- An explanation of what cyberbullying is
- An overview of the technologies employed by cyberbullies
- Tips on preventing its occurrence in schools
- Signs for parents, caregivers and teachers to look out for
- Advice to children on how to prevent and report cyberbullying
- Suggestions on how to sanction against cyberbullies
- An overview of the UK laws relevant to cyberbullying

The Cyberbullying Taskforce comprises members of a host of child welfare organisations, teaching unions and children's charities; educational organisations; ISPs; social network site providers; broadcasters; mobile operators; technology providers and technology experts, including the Cyberspace Research Unit from the University of Central Lancashire.

This document aims to provide senior managers and network administrators in schools, colleges and universities with a response to the DCSF Guidance outlining how M86 appliances and software can be used to combat cyberbullying perpetrated through email, Instant Messaging and Web use in schools. The M86 response does not cover cyberbullying undertaken via mobile phone or off the school network.

M86 acknowledges that while the Internet provides an incredibly rich resource for enhancing children's learning and social development, it can also be used to disseminate harmful information from individuals to a vast number of recipients and provide a gateway for viruses to enter the school's network. In particular the Guidance cites the use of email to forward bullying messages as a major factor in the perpetration of cyberbullying. It rightly points out that this act of forwarding messages can cause other pupils to unwittingly become "accessories" to the bullying, while increasing the distress felt by the subject of the email.

M86's response aims to restore students' and teachers' confidence in using ICT within their learning environment by outlining the technology that is available to combat misuse of the Internet, email and Instant Messages and keep the network secure. Internet and email-borne threats present serious challenges for organizations of all sizes and in all sectors. A multi-layered approach to Internet security is required.

1.2.2 Digital media, computer, mobile phones and the internet have been a taken-for-granted part of most children and young people's upbringing and environment. Many rely on technology not just to keep in touch, but as a way of developing their identities, socialising, and belonging to groups. "Technology can play a positive, productive and creative part of young people's activities, development and social participation." Source: Cyberbullying - safe to Learn: Embedding anti-bullying work in schools.

WHO IS M86 SECURITY?

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 24,000 customers and over 17 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

Specifically, M86 helps educational organizations of any size to:

- Secure networks from misuse and external threats
- Proactively enforce Internet use policies and reduce legal liabilities
- Protect students, staff, inbound and outbound information and the school's reputation
- Comply with legal requirements
- Optimize network bandwidth and improve productivity

SOFTWARE SOLUTIONS FOR EDUCATION

M86 MailMarshal Exchange—one of the few solutions available in the market today to provide email management that filters and manages internal inbox-to-inbox email for educational organizations. It monitors and controls internal office email content that travels within a school, college or university to ensure a safe, productive working environment and compliance with acceptable use policies.

M86 WebMarshal—the most complete secure Web gateway solution on the market today. It goes beyond URL filtering to provide comprehensive Web access control and management, complete threat protection (URL, AV and malware filtering) and data leakage prevention in a single, policy-based, easy-to-manage and highly scalable solution.

M86 MailMarshal SMTP—an email security solution that combines email threat protection, content security, policy enforcement, compliance and data leakage prevention into a highly scalable, flexible, easy-to-manage solution. M86 MailMarshal acts as an email gateway, powered by an unrivalled Defense-in-Depth Anti-Spam Engine, filtering all incoming and outgoing email at the network perimeter.

Marshal EndPoint Security—a policy-based enforcement solution that allows only authorized removable media devices to connect to school computers and servers, preventing data leakage and data theft. It enables educational organizations to monitor and control what information goes in and out of the school network via removable media devices such as USB flash drives, iPods, PDAs and CDs.

M86 MailMarshal Secure Email Server —a dedicated policy-based secure email solution that provides encryption, digital signing and deep content inspection of inbound and outbound email messages. It operates with any email gateway that can recognize S/Mime encrypted email, and automatically updates contact details and secure certificate credentials for encryption contact via a centralized server.

M86 MailMarshal Service Provider Edition—a SaaS security M86 solution enabling Managed Service Providers and Internet Service Providers to offer hosted email content security services to any size of school and small office/home office (SOHO) customers. It combines email filtering, anti-spam, anti-virus, anti-pornography, anti-phishing, policy compliance, email archiving and reporting into a centrally managed, highly scalable architecture.

HARDWARE SOLUTIONS FOR EDUCATION

M86 Web Filtering and Reporting Suite—a high-performance, scalable appliance-based Internet Security Suite, integrating best-in-class URL filtering, application control, detailed forensic reporting and real-time monitoring and mitigation of Web-based threats. The M86 Web Filtering and Reporting Suite is interoperable and easy to deploy in any network infrastructure—using M86's "Pass-by Technology" for zero network impact and fail-safe operation.

M86 MailMarshal e10000—an award-winning security appliance built upon the same platform and policy engine as M86 MailMarshal SMTP software that combines the ease of installation and low administration overhead of a hardware appliance with the flexibility, scalability and depth of functionality of a software solution.

DCSF DEFINITION OF CYBERBULLYING

"1. Cyberbullying can be defined as the use of information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target.

The Education and inspections Act 2006 (EIA 2006) includes legal powers that relate more directly to cyberbullying; it outlines the power of head teachers to regulate the conduct of pupils when they are off-site and provides a defence in relation to the confiscation of mobile phones and other items." – source: Cyberbullying - Safe to Learn: Embedding anti-bullying work in schools

Response to the DCSF Guidance:

What the Guidance States

4. Although cyberbullying is not a specific criminal offence, there are criminal laws that can apply in terms of harassment and threatening and menacing communications. Schools should contact the police if they feel that the law has been broken.

5. Cyberbullying takes different forms: threats and intimidation; harassment or “cyber-stalking” (e.g. repeatedly sending unwanted texts or instant messages); vilification / defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images (including what are sometimes misleadingly referred to as ‘happy slapping’ images); and manipulation.

6. Some cyberbullying is clearly deliberate and aggressive, but it is important to recognise that some incidents of cyberbullying are known to be unintentional and the result of simply not thinking about the consequences. What may be sent as a joke, may not be received as one, and indeed the distance that technology allows in communication means the sender may not see the impact of the message on the receiver. There is also less opportunity for either party to resolve any misunderstanding or to feel empathy. It is important that pupils are made aware of the effects of their actions.

7. In cyberbullying, bystanders can easily become perpetrators – by passing on or showing to others images designed to humiliate, for example, or by taking part in online polls or discussion groups. They may not recognise themselves as participating in bullying, but their involvement compounds the misery for the person targeted. It is recommended that anti-bullying policies refer to those ‘bystanders’ – better termed ‘accessories’ in this context – who actively support cyberbullying and set out sanctions for this behaviour. It is important that pupils are aware that their actions have severe and distressing consequences and that participating in such activity will not be tolerated.

8. It is important to decide on the roles and responsibilities for cyberbullying prevention work. This will typically involve a named lead from the senior management team (usually the person with overall responsibility for anti-bullying work), as well as IT staff, pastoral care staff, and school council members.

How M86 Products Help

M86’s email and web filtering products enable IT administrators at schools, colleges and universities to enforce acceptable use policies by blocking offensive content in emails, webmail, Instant Messages or web sites.

M86 can also be used to monitor any attempts to flout the school’s Acceptable Use Policy (AUP) so that evidence can be gathered.

M86 applies key words to monitor, filter and where necessary, block any email or Webmail containing derogatory, racist, sexist, pornographic or otherwise inappropriate content. This prevents the inadvertent sending or forwarding of emails that could cause the recipient to feel harassed, offended or distressed.

M86 Image Analyzer technology is used within industry to prevent the sending of pornographic email attachments.

Rules can be applied within M86 MailMarshal and M86 WebMarshal products to enable administrators to monitor images sent via the school’s network. This allows school staff to be alerted if a particular attachment is being forwarded to multiple recipients so that they can speak to the pupils concerned.

M86 products allow central administration of email and web traffic, so that acceptable use policies can be applied and enforced by the senior management team and IT staff at the school, college or university.

In addition, the reporting tools offered by M86 Security Reporter, provides a clear record of the school’s work to prevent cyber bullying as part of its overall eSafety strategy

Response to the DCSF Guidance:

What the Guidance States

11. It is advised that schools establish, or review existing Acceptable Use Policies (AUPs) referencing responsible use of school IT networks and equipment, Virtual Learning Environments (VLEs) and mobile phones. It is also recommended that schools review how the school network is monitored and check whether existing procedures are adequate.

12. It is recommended that schools record and monitor incidents of cyberbullying in the same way as all other forms of bullying. Schools can use this information to develop their policies and practices.

13. Publicising reporting routes is an important element of prevention, raising awareness of the issue but also ensuring that any incidents can be stopped before they become too serious or upsetting.

14. Education and discussion around the responsible use of technologies and e-safety are key to preventing cyberbullying and helping children and young people deal confidently with any problems that might arise, whether in or out of school. Technology can have a positive role in learning and teaching practice, and there is a need for staff to be confident about ICT in order to model the responsible and positive use of technologies and to respond to incidents of cyberbullying appropriately.

18. The person being bullied will usually have examples of texts or emails received, and should be encouraged to keep these to aid in any investigation. There are also additional reporting routes available, through mobile phone companies, internet service providers and social networking sites.

19. Some forms of cyberbullying involve the distribution of content or links to content, which can exacerbate, extend and prolong the bullying. There are advantages in trying to contain the spread of these, and options here include contacting the service provider, confiscating phones, and contacting the police (in relation to illegal content).

How M86 Products Help

Once the school's AUPs have been drawn up, M86 will enforce these across the network and monitor any attempts to bypass the AUP, enabling staff to nip cyberbullying incidents in the bud.

M86 products are used in the financial sector, police forces and government offices to guard corporate reputation and prevent staff from flouting AUPs deliberately or accidentally.

M86 provides central reporting tools that allow schools to monitor and record incidents that flout their AUP on email, instant messaging or Web use. These records can be used to demonstrate that the school is doing everything it can to safeguard their pupils' online learning environment.

M86's email, IM and Webmail monitoring allows for actual or suspected cyberbullying incidents to be flagged to staff, or blocked from being forwarded. This enables staff to intervene at an earlier stage to speak to the pupils involved and reinforce the school's teaching on cyberbullying.

M86 allows uses industry-proven technology to enforce the school's AUP on email, IM and Web use. This enables teaching staff to have confidence in using ICT as a teaching aid, without risking some pupils being exposed to Web threats or cyberbullying in the course of using the very ICT tools that were designed to enhance their learning.

M86's email, IM and Web filtering technology was designed to deliver enterprise-level monitoring and reporting. Used in an education environment, Mar86's appliances and software allow network managers in schools, colleges and universities to quickly generate reports of all web use and attempts to send emails or IMs that flout the school's AUP. This not only allows teachers to act swiftly to nip cyberbullying incidents in the bud, but also provides a valuable record of the school's eSafety strategy in action.

M86's content filtering technology enables key word lists to be created by a school's network administrator that subsequently flags, monitors or blocks emails, IMs or Webmail that appear to contain banned content. This prevents inappropriate content such as homophobic, racist, sexist or pornographic content from being forwarded from the school's network, or between network users.

Response to the DCSF Guidance:

What the Guidance States

21. Take steps to identify the person responsible for the bullying. Steps can include looking at the school system and computer logs; identifying and interviewing possible witnesses; and, with police involvement, obtaining user information from the service provider.

1.1.2 Cyberbullying is a sub-set or 'method' of bullying. It can be used to carry out all the different 'types' of bullying (such as racist bullying, homophobic bullying, or bullying related to special educational needs and disabilities), but instead of the perpetrator carrying out the bullying in person, they use technology as a means of conducting the bullying.

Cyberbullying can include a wide range of unacceptable behaviours, including harassment, threats and insults. And like face-to-face bullying, cyberbullying is designed to cause distress and harm.

1.1.3 Cyberbullying can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, cyberbullying does differ in several significant ways to other kinds of bullying: for example, the invasion of home/personal space; the difficulty in controlling electronically circulated messages; and even in the profile of the bully and target. These differences are important ones for people working with children and young people to understand (see section 1.4).

1.1.4 Cyberbullying takes place between children; between adults; but also across different age groups. Young people can target staff members or other adults through cyberbullying: there are examples of school staff being ridiculed, threatened and otherwise abused online. Research carried out for the Anti-Bullying Alliance (ABA) by Goldsmiths, for example, found that 22% of 11-16 year-olds had been a victim of cyberbullying¹.

- The MSN cyberbullying report (2006) found that 11% of UK teens had experienced cyberbullying².
- Noret and River's four year study on bullying (2007) found that 15% of the 11,227 children surveyed had received nasty or aggressive texts and emails, and demonstrated a year-on-year increase in the number of children who are being bullied using new technology.
- Research conducted as part of the DCSF cyberbullying information campaign found that 34% of 12-15 year olds reported having been cyberbullied.
- Qualitative evidence gathered by NASUWT through a survey of teachers has demonstrated that cyberbullying affects the working lives of staff and impacts severely on staff motivation, job satisfaction and teaching practice.

How M86 Products Help

M86's content filtering and reporting technology can rapidly reconstruct Internet access and allow school network administrators to quickly drill down into log data to track individual's Web and email activity.

M86 allows management to look at Web pages, search categories and graphics accessed.

Where cyberbullying has been occurring over a sustained period, M86 MailMarshal and M86 WebMarshal allow key words to be set up to trap or flag subsequent email or webmail messages containing particular file types — words or syntax.

M86 MailMarshal Exchange is an internal email filtering solution for Microsoft Exchange Server 2000 / 2003 / 2007. It provides email content analysis and acceptable use policy enforcement and reporting technologies in a single, easy to manage solution.

M86 MailMarshal Exchange can also integrate with optional modules for anti-virus scanning, anti-spyware and pornographic image detection.

M86 MailMarshal Exchange acts as a plug-in to Microsoft Exchange Server, applying full content inspection and policy enforcement to all email flowing through Exchange. This ensures that all messages passing between mailboxes, or Exchange servers in remote offices, is legitimate and complies with acceptable use policies.

M86 MailMarshal and M86 WebMarshal can help educational institutions meet their legal obligations by blocking access to inappropriate web sites and blocking email messages containing offensive language.

M86 solutions can block access to prohibited chat rooms and web sites, M86 WebMarshal can help educational institutions meet their legal obligations by blocking access to inappropriate web sites and Instant Messaging. M86 MailMarshal Exchange can do so by blocking internal email containing offensive language.

Response to the DCSF Guidance:

What the Guidance States

1.2.4 Barring or restricting school network access to particular sites that young people use, such as social networking and gaming sites, does not necessarily prevent young people from using them. They will still access them, via their own devices and connections, by bypassing blocks, or by finding new, unrestricted sites. Whatever policies and practices individual schools might have around computer access, mobile phones, or game consoles, it is important to recognise how important technology is to young people. Education and discussion around responsible use and e-safety is key to helping them deal confidently with any problems that may arise, whether in or out of school. Adults are not always aware of how technologies can be used and abused.

1.2.7 As technology develops, children will be experimenting with new environments and exploring where the boundaries of behaviour lie. In order to engage in a discussion about acceptable and responsible use, it is necessary to be informed about these technologies, in order to help identify where the limits are and what the potential impacts of certain behaviours are. It is not necessary to know about every application or site – but it is important to keep up to date with a broad understanding of the different ways that young people are using or abusing technologies.

1.3.5 Cyberbullying can include posting upsetting or defamatory remarks about an individual online, or name-calling using a mobile device for example. These may be general insults, or include prejudice-based bullying. Pupils may use their mobile phones or email to send sexist, homophobic and racist messages, for example, or they may attack other kinds of difference – a physical or mental disability, cultural or religious background, appearance, or socio-economic position.

1.4.6 Bystanders to cyberbullying can easily become perpetrators – by passing on or showing to others an image designed to humiliate another child or staff member, for example, or by recording an assault/act of bullying on a mobile phone and circulating this.

As with other forms of bullying, it is important that the whole-school community understands their responsibility to report cyberbullying and support the person being bullied. It is advisable that anti-bullying policies refer to those ‘bystanders’ – better termed ‘accessories’ in this context – who actively support cyberbullying incidents and set out sanctions for this behaviour.

How M86 Products Help

M86 proxy blocker technology is able to prevent one of the most common techniques employed by students to bypass Web filters and access prohibited web sites.

M86 WebMarshal allows school administrators to set up “whitelists” of approved Web sites that students can access.

In one school, M86’s technology alerted staff to a female pupil who was trying to bypass controls to access sites under the search term “sexual abuse”. When staff intervened they were able to establish that the pupil had suffered abuse and refer her to a professional counsellor.

M86 security solutions prevent students from using proxy sites to bypass school Web filters that are designed to prevent them from accessing unsuitable web sites from the school network.

M86 MailMarshal Exchange monitors and controls internal email content sent within a school, college or university to ensure a safe, productive working environment and compliance with acceptable use policies.

M86 MailMarshal enforces AUP by enabling lists of key words to be monitored to prevent racist, homophobic, sexist or other derogatory language being sent via the school’s email network

The data leakage prevention technology within M86 MailMarshal and M86 WebMarshal looks for certain keywords or content and prevents messages being forwarded if they contain “suspect” content. This allows school network administrators to flag where AUPs have been flouted so that teaching staff can intervene to nip the incident in the bud by speaking to the students concerned.

This prevents the misery of cyberbullying being compounded through “bystanders” forwarding on messages contain defamatory information or humiliating images.

Response to the DCSF Guidance:

What the Guidance States

1.4.11 Perpetrators are not as anonymous as they might think and there are ways of identifying cyberbullies.

Having said that, although there is likely to be an evidence trail ('digital footprints') left by the bully, finding out further information that might help identify who is responsible – by tracking down the person's email or IP address (their unique computer address) – is time consuming and usually requires the involvement of other agencies (the police and the service provider, for example). And in some cases, finding out this information will not clearly identify an individual.

1.4.12 Some cyberbullying is clearly deliberate and aggressive. However, some instances of cyberbullying are known to be unintentional and the result of not thinking or a lack of awareness of the consequences. Online behaviours are generally less inhibited than offline behaviour, and some children report saying things to others online that they would not have done offline. Two other factors may be involved here:

- The distance between the bully and the person being bullied: The lack of context can mean that what might intended as a joke may not be received as such, and indeed may be deeply upsetting or offensive to the recipient. Additionally, because the bully cannot see the person being bullied, and the impact that their message has had, there is less chance for either to resolve any misunderstanding or to feel empathy.
- A single act can have unintended consequences: Sending a 'funny' (i.e. embarrassing or humiliating) picture of a fellow pupil (even a friend) to someone could be viewed as a one-off incident, but the nature of the technology means that the sender loses control of the image they have sent. It can be sent on, posted up online and have a wide circulation. For this reason, a one-off action can turn into a repetitive action, and have consequences for the person being bullied far beyond what the original sender may have anticipated.

How M86 Products Help

M86 products were designed to enable management and monitoring of electronic communications to enable compliance with industry regulations. The centralised reporting offered by M86 MailMarshal, M86 WebMarshal and M86 Web Filtering and Reporting Suite deliver detailed forensic reporting and real-time monitoring.

Importantly, M86 products achieve this monitoring without impacting on network performance, even when a single appliance is supporting up to 30,000 end users on a local education authority network.

M86 products were designed to reduce the risk from Web and email use and prevent data loss. When applied to an educational environment, this allows network administrators to set up rules that prevent pupils from forwarding emails or Webmails containing prohibited content.

This prevents pupils from inadvertently taking part in a cyberbullying incident by forwarding messages that were designed to cause distress to an individual.

Response to the DCSF Guidance:

What the Guidance States

1.4.13 Schools need to ensure that ignorance of the consequences and potential seriousness of cyberbullying is not a defence – that all pupils are aware of the issues and rules, for example through induction procedures, awareness days and Acceptable Use Policies

1.5.3 Instant messenger (IM) is an application that allows the pupil to chat in real time (i.e.live) with people on a pre-selected friend/buddy list. IM programmes usually require you to download an application to your computer, although there are some web-based services available which do not need installing. IM and bullying.

Bullies can use IM to send nasty messages or content to other users. People can also ‘hack’ into IM accounts and send nasty messages to contacts.

How M86 Products Help

How M86 helps with enforcement of Acceptable Use Policies against Inappropriate Content

Whether an educational institution is teaching primary school-age children or university students, they all have strict standards on how learning and communication tools (like email and the Internet) can be used.

Common requirements include prohibition of pornography, profanity, racist or hate content and other inappropriate content.

Universities and colleges often take a proactive approach to issues such as harassment and racism by banning the use of certain words in email.

M86 MailMarshal and M86 WebMarshal can help educational institutions meet their legal obligations by blocking access to inappropriate web sites and blocking email messages containing offensive language. M86 MailMarshal and M86 WebMarshal are completely flexible, allowing faculty members to access different types of web or email content to that permitted to students.

M86 MailMarshal with Image Analyzer can detect and block pornographic images attached to emails. This makes it possible to control the sharing of pornography in an email environment. M86 WebMarshal not only blocks access to pornographic web content, but also establishes whitelists of approved content and limits student access to these approved web sites.

M86 WebMarshal allows school network administrators to control web applications including instant messaging and streaming media. M86 WebMarshal 6.1 enables the most granular policies to be enforced to control access to encrypted HTTPS sites. HTTPS content scanning ensures that users can only use secured sites that meet approved standards; and that all content flowing in and out of a school's network conforms to internal policies.

Schools can also use M86 WebMarshal to implement policies to allow, or block, a range of streaming video protocols, including Apple QuickTime Audio/Video (RTSP), Google Video, Microsoft Windows Media, Real Media and YouTube.

Instant Messaging can also be explicitly allowed or blocked; supported Instant Messaging systems include, AOL Instant Messenger (AIM), Google Talk, Windows Live Messenger and Yahoo! Messenger

Response to the DCSF Guidance:

What the Guidance States

Email and bullying

Email can be used to send inappropriate images and to forward private information. Computer viruses and spam are common email hazards. Web-based email can also be used by people wanting to remain anonymous in order to send malicious or nasty mail.

People can send bullying or threatening messages via email, or repeatedly send unwanted messages. Unsuitable images or video clips can be passed on. Personal emails can be forwarded inappropriately. The majority of computer viruses are forwarded by email.

2.1.6 There is no single solution to the problem of cyberbullying; it needs to be regarded as a live and ongoing issue. This section outlines a prevention framework made up of the five essential action areas that together offer a comprehensive and effective approach to prevention:

- Understanding and talking about cyberbullying
- Updating existing policies and practices
- Making reporting cyberbullying easier
- Promoting the positive use of technology
- Evaluating impact of prevention activities

2.3.1 Review and update policies to include cyberbullying

2.3.3 The school's anti-bullying policy and/or school behaviour policy will certainly need to address cyberbullying if they do not already do so. It is important too that cyberbullying is addressed in ICT and other relevant lessons, and is brought to life through activities. As with other whole-school policies, it is important to include and empower young people to take part in the process.

How M86 Products Help

M86 MailMarshal applies full content inspection and AUP enforcement to all email. By setting up an agreed list of inappropriate and prohibited language, emails containing sexist, racist or derogatory language can be blocked or monitored to allow early staff intervention.

This enables schools to provide a safe learning environment for pupils— safe from harassment and offensive messages. M86 MailMarshal also helps increase productive study time by blocking distracting or malicious email content and attachments.

M86 MailMarshal is designed to block spam, malware and inappropriate content. Its Image Analyzer technology allows for deep content inspection of all messages passing through the SMTP gateway or Exchange server to block, flag and audit any messages that contravene AUPs.

M86 products are policy-based and designed to help educational organizations reduce the administrative burden of monitoring email and Web use by automatically enforcing Acceptable Use Policies. These can be updated as necessary, to reflect changes in the school's policy or government guidance regarding cyberbullying.

M86 Security Reporter provides school network administrators with detailed forensic reporting on Web use. M86 WebMarshal 6.1 provides additional management tools with a real-time dashboard, giving a dynamic view of recent Web traffic activity and system performance and providing administrators with an indispensable monitoring and reporting tool.

M86 products are policy-driven and can be used as a powerful component in a school's eStrategy by enforcing AUPs regarding Internet, IM and email use in an effort to minimise abuse of these resources.

By enforcing the school's AUPs on email and Web use, M86 products create a safe online environment. This helps instil confidence in ICT and promotes the positive use of technology by pupils.

Response to the DCSF Guidance:

What the Guidance States

Log all cyberbullying incidents

2.3.4 Keeping good records of any incidents of cyberbullying is essential, and can help to monitor the effectiveness of your school's prevention activities. The use of technology in any incident can be recorded using your existing incident report forms and these can be logged as cyberbullying incidents.

2.4.4 Because reporting can be difficult, it is important to have different ways for reporting cyberbullying incidents. Making reporting as easy as possible, and making sure everyone knows how they can report incidents is also an excellent way of raising awareness that cyberbullying is unacceptable.

Review your existing Acceptable Use Policies (AUPs) 2.3.5 AUPs are the rules that students have to agree to follow in order to use ICT in school. If you only have these online, you might want to produce a paper form that can be sent home for parents to see.

You may want to produce separate AUPs for using different kinds of technology – e.g. for use of the school network; use of a school Virtual Learning Environment (VLE) or other learning platforms / interactive tools; and use of mobile phones on school premises. Policies should outline the rules and responsibilities of use, sanctions for misuse, and issues around confiscation and retention.

2.5.10 The ability to conduct searches of internet use records at school is an important part of being able to investigate incidents of cyberbullying. Your school may want to review and investigate available software, for example monitoring software and key logging programmes. It is important that learners are aware of what monitoring procedures are in place. Knowing that the school is taking such steps may also act as a disincentive for bullies to misuse school equipment and systems. However, it is important to remember that using technology to monitor, block or filter activity at school is only a partial solution.

How M86 Products Help

The M86 MailMarshal Reporting Console is a Web-based reporting suite that offers a comprehensive set of reports on content filtering and monitoring of email policy enforcement for all email traffic at the gateway to the school's network. The M86 Security Reporter provides school network administrators with detailed forensic reporting on Web use. M86 WebMarshal 6.1 offers a real-time dashboard that provides a dynamic view of recent Web traffic activity and system performance.

M86 allows for granular enforcement of AUPs with the flexibility to update filtering rules whenever the school's AUPs are reviewed.

M86 offers advanced reporting features that log all Web and email activity against AUPs, creating a valuable report of online activity for all users on the network.

If a pupil attempts to "shadow surf" or use proxy servers to bypass the school's web filters, this will be blocked and a message displayed on the pupil's screen reminding them that their activity contravenes the school's AUPs.

Similarly, if a pupil tries to send or forward an attachment containing inappropriate content, or send an email containing bullying language, a message will be displayed explaining why their message has been blocked. This is often a sufficient deterrent for the less determined bully. However, policy-based content filtering technology must be used in conjunction with staff vigilance and intervention.

Response to the DCSF Guidance:

What the Guidance States

2.6.3 The Children's Commissioner has recommended that all schools conduct an annual survey of pupil's experiences of bullying. Cyberbullying incidents could be included in such a survey. This will provide schools with a good overview of how common cyberbullying incidents are amongst pupils, and highlight any areas that need particular attention. It will also provide you with a broad measure against which you can check the progress and impact of your prevention activities

3.2.3 It is important to advise the person being bullied not to retaliate or return the message. Replying to messages, particularly in anger, is probably just what the bully wants, and by not replying the bully may think that the target did not receive or see the message, or that they were not bothered by it. Instead, the person should keep the message as evidence.

3.4.7 In addition to any sanctions that are in existing anti-bullying / behaviour policies, it is important to refer to any Acceptable Use Policy or agreement for internet and mobile use, and apply sanctions for breaches where applicable and practical. The best way to deal with cyberbullying is to prevent it happening in the first place. Although it may be uncomfortable to accept, you should be aware that your child may as likely cyberbully as be a target of cyberbullying and that sometimes children get caught up in cyberbullying simply by not thinking about the consequences of what they are doing. It is therefore crucial that you talk with your children and understand the ways in which they are using the internet and their mobile phone.

How M86 Products Help

The M86 MailMarshal Reporting Console is a Web-based reporting suite that offers a comprehensive set of reports on content filtering and monitoring of email policy enforcement for all email traffic at the gateway to the school's network

M86 Security Reporter provides school network administrators with detailed forensic reporting on Web use.

M86 WebMarshal 6.1 offers a real-time dashboard that provides a dynamic view of recent Web traffic activity and system performance.

M86 monitoring solutions enable tracking of individual user records to gather evidence of cyberbullying.

M86 products were designed to provide enterprises with the peace of mind that company data was not being shared over email or Webmail in contravention of company AUPs or legal requirements.

When applied to an educational environment, this policy-based enforcement provides a robust solution to preventing cyberbullying over a school's Internet and email system.

Cyberbullying and the Law:

What the Guidance States

In fact some cyberbullying activities could be criminal offences under a range of laws including:
Protection from Harassment Act 1997
Section 127 of the Communications Act 2003
The Malicious Communications Act 1988, Section 1 makes it an offence to send indecent, grossly offensive or threatening letter, electronic communication or other article to another person with the intention that it should cause them distress or anxiety

The Public Order Act 1986
The Obscene Publications Act 1959
www.opsi.gov.uk/acts/acts1997/1997040.htm
www.opsi.gov.uk/acts/acts2003/20030021.htm
www.opsi.gov.uk/ACTS/acts1988/Ukpga_19880027_en_1.htm
www.opsi.gov.uk/si/si1987/Uksi_19870198_en_2.htm

1.3.15 Creating, possessing, copying or distributing images of children and young people under the age of 18 which are of an indecent or sexual nature is illegal under the Protection of Children Act 1978. These images are illegal even if they were taken in 'fun' or by 'willing' parties. Section 160 of the Criminal Justice Act 1988 criminalizes the possession of electronic or hardcopy images. These laws also apply to indecent 'pseudo-photographs'— images which have not been taken but have been created or adapted, for instance using digital imaging software.

An anti-social behaviour order (ASBO) under the Crime and Disorder Act 1998 could be used for cyberbullying. An ASBO is a civil order which prohibits an individual from engaging in specific anti-social acts. An ASBO can be made against any person, aged 10 years or over, where there is evidence that their behaviour caused, or is likely to cause, harassment, alarm or distress to others and where an order is needed to protect person(s) from further anti-social acts. An ASBO can be used in conjunction with other measures as part of a tiered approach to tackling anti-social behaviour. Prohibitions should be precise, targeted at the specific behaviour complained of, and proportionate to the legitimate aim of protecting the community from further abuse. ASBOs can be extremely effective in preventing further escalation into criminal behaviour. Breach of an Anti-Social Behaviour Order is a criminal offence and criminal penalties apply.

How M86 Products Help

Issues such as bullying, sexual harassment, racism, copyright, pornography, incitement of religious hatred and chat room predators mean that educational institutions are required to take every reasonable and practical step to protect children in their charge.

M86 solutions allow teaching and IT staff to monitor and control all of these issues to the highest legal standards and to deal immediately with any issues that might arise.

M86 solutions can block emails and Webmails containing prohibited words or offensive content and prevent access to pornographic web sites and prohibited chat rooms.

M86 solutions provide a significant component in a school's eSafety strategy and help schools comply with legal requirements.

M86 MailMarshal Exchange enables educational establishments to meet their obligations to provide a safe learning environment for students and staff—free from harassment and objectionable material. It also helps prevent students from spending valuable lesson time "off task" by managing email content and attachments.

GUIDANCE ON ACCEPTABLE USE POLICIES

An example of an acceptable use policy for use in schools can be downloaded from:

www.teachernet.gov.uk/publications

The guidance document, "Cyberbullying - Safe to Learn: Embedding anti-bullying work in schools," developed in consultation with the Department for Children, Schools and Families (DCSF) Cyberbullying Taskforce, can also be downloaded from this site:

Search using the ref: DCSF-00658-2007

Copies of "Cyberbullying - Safe to Learn: Embedding anti-bullying work in schools" can also be obtained from:

DCSF Publications
PO Box 5050
Sherwood Park
Annesley
Nottingham NG15 0DJ
Tel: 0845 60 222 60
Fax: 0845 60 333 60
Textphone: 0845 60 555 60

Please quote ref: 00658-2007DOM-EN

ISBN: 978-1-84775-028-0

PPBEL/D21/0907/53

Excerpts from the document have been reproduced under the terms of the Click-Use Licence.

ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 24,000 customers and over 17 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advance threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters

828 West Taft Avenue
Orange, CA 92865
United States
Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific

Millennium Centre, Bldg C, Level 1
600 Great South Road
Ellerslie, Auckland, 1051
New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 04/19/10