MONKWEARMOUTH ACADEMY

E-Safety Policy

Rationale

The purpose of this policy is to:

- Set out the key principles expected at the academy of all members of the academy community with respect to the use of ICT-based technologies
- Safeguard and protect the children and staff of the academy
- Highlight issues affecting the use of ICT based communication systems
- Assist academy staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other academy policies
- Ensure that all members of the academy community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Minimise the risk of misplaced or malicious allegations made against adult who work with students
- State the actions that may be taken to monitor the effectiveness of this policy
- Warn users about the consequences of inappropriate use of ICT-based technology and systems

The main areas of risk for our academy community can be summarised as follows:

<u>Content</u>

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games and substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites, including online radicalisation
- Content validation, how to check authenticity and accuracy of online content

<u>Contact</u>

- Grooming
- Cyber-bullying in all forms
- Identity theft including 'frape' (hacking Facebook profiles), other social media hacking and sharing passwords.

<u>Conduct</u>

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and wellbeing (amount of time spent online)
- Sexting (sending and receiving of personally intimate images)
- Copyright

Scope

This policy applies to all members of the academy community (including staff, contractual third parties and all agents of the academy, students, volunteers, parents/carers, visitors and community users) who have access to and are designated users of the academy ICT systems, both in and out of the academy, including remote access. The use of ICT facilities by staff not authorised will be regarded as a disciplinary offence.

It covers all ICT facilities and communication systems provided by the academy for the purpose of conducting and supporting official business activity through the academies network infrastructure and all stand alone and portable computer devices.

The Education and Inspections Act 2006 empowers Headteachers, to such an extent as is reasonable, to regulate the behaviour of students when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, radicalisation or other e-safety incidents covered by this policy, which may take place outside the academy, but is linked to membership of the academy.

The Education Act 2011 increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issued covered by the published Academy Behaviour Policy.

The Academy will deal with such incidents within this policy and associated anti-bullying and behaviour policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that takes place outside of the academy.

Staff and students have a responsibility to report any instances of witnessing or discovering blocked online searches or sharing of extremist or bullying messages or social profiles.

Any material/activity that the academy believes is illegal will be reported to the appropriate agencies including the police and CEOP.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named **e-safety co-ordinator** in our academy is **Michael Grummett**, **Deputy Headteacher** who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the e-safety co-ordinator to keep abreast of current issues and guidance through organisations such as Sunderland LA, Safeguaridng First and CEOP (Child Exploitation and Online Protection).

SLT and Governors are updated by the e-safety co-ordinator and all governors have an understanding of the issues and strategies at our academy in relation to local and national guidelines and advice.

This policy, supported by the academy's acceptable use agreements for staff, governors, visitors and students (appendices), is to protect the interests and safety of the whole school community. It is linked to the following policies: child protection, teaching and learning, health and safety, safer working practices, home–school agreements, disciplinary, staff behaviour policy, anti-bullying and behaviour and discipline**.**

Our staff receive regular information on e-safety issues in the form of briefing notes and policy guidance, whole staff training is also delivered.

New staff receive information on the academy's acceptable use policy as part of their induction.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Policy Compliance

If any user is found to have breached this policy, they may be subject to the academy's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender.

If you do not understand the implications of this policy or how it may apply to you, seek advice from Mr P Moorhead or Mr M Grummett.

- Users must familiarise themselves with the detail of this policy before using any of the academy ICT facilities on or off site
- It is the user's responsibility to use all computer devices in an acceptable way. This includes not installing software that has not been approved, taking due care and attention when transporting and storing the equipment and not emailing CONFIDENTIAL information to a non-academy email address unless encrypted.
- Users should be aware of the physical security dangers and risks associated with working with ICT equipment offsite.
- Whilst respecting the privacy of authorised users, the academy maintains the legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of removable media by authorised users to ensure adherence to this policy.
- In addition to routine monitoring and audits, where a manager suspects that academy ICT equipment is being abused or misused by a user, they should inform their line manager. Should an investigation be authorised, designated staff may carry out an internal audit.
- In addition, the academy will comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for information.

Applying the Policy

All IT equipment (including portable computer devices) supplied to users is the property of the academy. It must be returned upon the request of the academy.

All IT equipment will be supplied and installed by the academy IT staff. Hardware and software must only be provided by the academy.

Student E-safety Curriculum

This academy has a clear, progressive e-safety education programme as part of the curriculum which covers a range of skills and behaviours appropriate to age and experience, including,

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy
- to be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be
- to know how to narrow down or refine a search
- to understand how search engines work and to understand that this affects the results they see at the top of the listings
- to understand acceptable behaviour when using an online environment/e-mail, ie be police, no bad or abusive language or other inappropriate behaviour and keeping personal information private
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- to understand why 'on-line' friends may not be who they say they are and to understand why they should be careful in online environments
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned on privacy settings
- to understand why they must no post pictures or videos of others without their permission

- to know not to download any files eg music files without permission
- to have strategies for dealing with receipt of inappropriate materials
- to understand why and how some people will 'groom' young people for sexual reasons
- to understand the impact of cyber-bullying, sexting, and trolling and know how to seek help if they are affected by any form of online bullying
- to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies
- to plan internet use carefully to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas
- to remind students about their responsibilities through an end-user ICT Acceptable Use Agreement, which every students will sign and will be displayed throughout the academy
- To ensure staff will model safe and responsible behaviour in their own use of technology during lessons
- To ensure that, when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights
- To ensure staff and students understand the issues around aspects of the commercial use of the internet as age appropriate. This may include risks in pop ups, buying online, online gaming/gambling and SPAM email.

Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. Students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are reminded regularly of the need for password security and required termly to change their log in password.

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the academy's e-safety Policy.

Users are provided with an individual network, email, Monkwearmouth Gateway and VLE log-in username.

Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

If you think your password may have been compromised or someone else has become aware of your password report this to the Network Manager**.**

Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)

In our academy, all ICT password policies are the responsibility of the Network Manager, Mr Moorhead**,** and all staff and students are expected to comply with the policies at all times.

Data Security

The accessing and appropriate use of academy data is something that the academy takes very seriously.

Staff are aware of their responsibility when accessing academy data. Levels of access are determined by the Executive Headteacher**.**

Data can only be accessed and used on academy computers, laptops or via the school gateway. Staff are aware they must not use their personal devices, memory sticks or portable hardrives for accessing any academy or student data.

Internet Access, Security and Filtering

This academy:

- Has educational filtered secure broadband connectivity through Durham and so connects to the 'private' Monkwearmouth Academy
- Uses Smoothwall filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, social media sites
- Uses Smoothwall user-level filtering where appropriate, thereby closing down/opening up options appropriate to the age/stage of students
- Ensures network health through protection, anti-virus software and network set up
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved learning platform
- Works in partnership with our providers to ensure any concerns about the systems are communicated so that systems remain robust and protect students
- Is vigilant in its supervision of students and staffs use at all times, as far as is reasonable
- Ensures staff and students sign an ICT Acceptable Use Agreement form and understand that they must report any concerns
- Ensures students only publish within an appropriately secure environment namely the academy's learning environment
- Requires staff to preview websites before use, plan the curriculum content for internet use to match students ability using child-friendly search engines eg Google Safe Search
- Is vigilant when conducting 'raw' image searches with students
- Informs all users that internet use is monitored
- Informs staff and students that they must report any failure of the filtering systems directly to the Network Manager
- Provides advice and information on reporting offensive materials, abuse/bullying etc available for students, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities eg the police.

Network Management

To ensure the network is use safely, this academy:

- Ensures staff read and sign to say that they have understood the academy's e-safety policy suite.
- Staff access to the network, internet, email and management information system is controlled via a username and password
- We provide with students with an individual network username and personal password
- Makes clear that no one should log on as another user and makes clear that students should never be allowed to log on or use teacher and staff logins
- Has set up the network with separate work areas for students and staff
- Requires all users to always log off/lock the workstation when they have finished working or are leaving the computer unattended.
- Scans all mobile equipment with anti-virus software before it is connected to the network.
- Maintains equipment to ensure health and safety is followed
- Has integrated curriculum and administration networks but access to management information systems is set up to ensure staff users can only access modules related to their role
- Our wireless network is secured to standards suitable for educational use.

Managing e-mail

The use of email within most schools is an essential means of communication for both staff and students. In the context of the academy, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level 4 or above, students must have experienced sending and receiving emails.

The academy gives all staff their own email account to use for all academy business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

It is the responsibility of the Network Manager in conjunction with each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.

Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses.

E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on academy headed paper.

Students may only use academy approved accounts on the academy system and only under direct teacher supervision for educational purposes.

Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

Staff must inform the e safety co-ordinator or Network Manager if they receive an offensive e-mail.

Students are introduced to email as part of the ICT Scheme of Work.

Safeguarding from Radicalisation

The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems in the academy blocks inappropriate content, including extremist content.

The academy has safeguards in place to filter out radicalisation through social media. Searches and web addresses are monitored and the Network Manager will alert senior staff where there are concerns and prevent further access when new sites that are unblocked, are found.

Where staff, students or visitors find unblocked extremist content they must report it to the Network Manager or the e-safety co-ordinator.

Any material that the academy believes is illegal will be reported to the appropriate agencies eg the police and CEOP.

Social Networking

For their own security employees should regularly review their privacy settings on all their social networking sites ensuring they have opted for the highest privacy settings on their account to minimise risks to themselves and the academy regarding reputation an professional integrity; however all communication via

social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider that that originally intended.

Staff must not access social networking sites for personal using the Academy's equipment.

Staff must not accept students as friends and are advised not to be friends with recent students and if a member of staff receives a message on their social networking profile that they think could be from a student they must report it immediately to their line manager.

Staff are advised not to write about their work, they must not disclose any information that is confidential to the Academy or information not yet in the public arena and should not make any defamatory remarks about the academy, colleagues or students.

The Academy endeavours to deny access to social media sites to students within the academy and all students are advised to be cautious about the information given by others on sites for example users not being who they say they are.

Students are taught through regular assemblies and social studies to avoid placing images of themselves (or others) on such sites and to consider the appropriateness of all images. Students are always reminded to avoid giving out personal details on such sites which may identify them and where they are.

Students are advised to set privacy settings to maximum levels and deny access to unknown individuals.

Personal Mobile devices (including phones)

The academy allows staff to bring in personal mobile phones and devices for their own use, however, this should not happen in a classroom setting or whist supervising students around the building. Under no circumstances does the academy allow a member of staff to contact a student or parent/carer using their personal device.

Students are allowed to bring personal mobile devices/phones to the academy, however, at all times the device must be switched off and out of sight. Under no circumstances may they be used on the premises. Any student found to be infringing this police will have their mobile phone confiscated and returned at the end of the day. The second confiscation will result in the student's phone being placed in the safe overnight and collected the next evening. Alternatively parents can come to the school office to collect the phone. Any subsequent confiscations will result in the student being unable to retrieve their phone themselves and the parent/carer being contacted to collect the phone.

The academy is not responsible for the loss, damage or theft of any personal mobile device.

Permission must be sought from the Designated Safeguarding Lead, Mr Graham before any image or sound recordings are made on these devices of any member of the school community.

Users bringing personal devices into the academy must ensure there is no inappropriate or illegal content on the device.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of students) and staff, the academy permits the appropriate taking of images by staff and students with **academy equipment.**

Staff are not permitted to use **personal digital equipment**, such as mobile phones and cameras, to record images of students, this includes when on field trips. However with the express permission of the Designated Safeguarding Lead, images can be taken provided they are transferred immediately and solely to the academy's network and deleted from the staff device.

Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

Publishing student's images and work

On a child's entry to the academy, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the academy web site
- on the academy's VLE
- in the academy prospectus and other printed publications that the academy may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the academy's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the academy
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the student attends this academy unless there is a change in the student's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Website Manager, Aaron Scott has authority to upload to the site.

Storage of Images

Images/ films of children can only be stored on the academy's network. Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Designated Safeguarding Lead.

Rights of access to this material are restricted to staff and students within the confines of the academy network.

The Network Manager has the responsibility of deleting the images when they are no longer required, or the student has left the academy.

Misuse and Infringements

Complaints

Complaints relating to eSafety should be made to the e-safety co-ordinator or the Designated Safeguarding Lead. Incidents should be logged and the academy procedure Managing an eSafety Incident should be followed.

Inappropriate material
All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety co-ordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety Co-ordinator, depending on the seriousness of the offence this may lead to; investigation by the Designated Safeguarding Lead/HR & Business Manager**,** referral to the Local Authority Designated Officer, possible disciplinary investigation and involvement of police for very serious offences.

This policy was updated in May 2017 and will be reviewed every 2 years or earlier if necessary.

Signed_____ Executive Headteacher Date_____

Signed _____ Chair of Governors Date_____

APPENDIX 1

Acceptable Use Agreement:

Staff, Governor and Visitor

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in the academy. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr Grummett, e-Safety coordinator.

- I will only use the academy's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' in line with the Staff Behaviour Policy.
- I will comply with the ICT system security and not disclose any passwords provided to me by the academy or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to students.
- I will only use the approved, secure email system(s) for any academy business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in the academy, taken off the academy premises or accessed remotely. Personal data can only be taken out of the academy or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of Paul Moorhead, Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes in line with academy policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the academy network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in the academy and outside of the academy, will not bring my professional role into disrepute.
- I will support and promote the academy's e-Safety policy and help students to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the academy.

Signature …….…… Date ……

Full Name ……..(printed)

Job Title……..

APPENDIX 2

Acceptable Use Agreement:
Student

- I will only use ICT systems in the academy, including the internet, email, digital video, mobile technologies, etc. for academy purposes.
- I will not download or install software on academy technologies.
- I will only log on to the academy network/ Learning Platform with my own user name and password.
- I will follow the academy's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my academy email address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project and is organised and approved by my teacher.
- I will report any unpleasant material or messages sent to me.
- Images of students and/ or staff will only be taken, stored and used for academy purposes in line with academy policy and not be distributed outside the academy network without the permission of the Network Manager, Mr Moorhead**.**
- I will ensure that my online activity, both in the academy and outside of the academy, will not cause my academy, the staff, students or others distress or bring into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, academy sanctions will be applied and my parent/ carer may be contacted.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the academy

Signature …….. Date ……

Full Name ……..(printed)

Tutor Group……..

APPENDIX 3

Academy logo and details

Dear Parent/ Carer

ICT including the internet, learning platforms, email and mobile technologies have become an important part of learning in our academy. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of eSafety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or Mr Grummett, e-safety Coordinator.

By signing this form parents/carers are agreeing to the following:

- Giving permission for their child to have access to the internet and to ICT systems at school
- Acknowledging that their child has signed an acceptable use agreement and will receive e-safety as part of their education at Monkwearmouth Academy
- Acknowledging that the Academy will take every reasonable precaution, including monitoring and filtering systems to ensue students will be safe when accessing internet and IT systems.
- Understanding that the Academy cannot ultimately be held responsible for the nature and content of materials accessed on the internet and mobile technologies.
- That student's activity on IT systems will be monitored and the school will contact parents/carers if there are concerns about any possible breaches of the acceptable use agreement.
- To encourage your child to adopt safe use of the internet and digital technologies at home and to inform the academy if you have concerns over your child's e-safety.

Please return the bottom section of this form to the academy for filing.

✂ -

Student and Parent/ carer signature

We have discussed this document and ……………………………….........(student name) agrees to follow the e-safety rules and to support the safe and responsible use of ICT at Monkwearmouth Academy.

Parent/ Carer Signature ……………………..…………………….

Student Signature………………………………………………….

Form …………………………. Date ……………………….

APPENDIX 4

E-Safety Useful Links and Resources

Parent Info – Expert information to help children and young people stay safe online http://parentinfo.org

CEOP (Child Exploitation and Online Protection Centre) – https://ceop.police.uk/safety-centre/

Think U Know – Provides the latest information on the sites you like to visit, mobiles and new technology. Find out what's good, what's not and what you can do about it. If you look after young people there are resources you can use in the classroom or at home. There is also a place which anyone can use to report if they feel uncomfortable or worried about someone they are chatting to online – www.thinkuknow.co.uk

Childline – Advice and support for children and young people – www.childline.org.uk

Internet Watch Foundation (IWF) – UK hotline for reporting criminal online content www.iwf.org.uk

UK Safer Internet Centre – Summarised research on e-safety – www.saferinternet.org.uk/research
Education packs – www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals

Digital Parenting Magazine – Online e-safety resources for parents – www.vodafone.com/content/parents.html

Digital Me – Safe – Safe is a programme of practical activities that develop young people's skills, self-confidence and safety awareness when using social networking sites – www.digitalme.co.uk/safe

UK Council for Child Internet Safety (UKCCIS) – www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Government Guidance – Radicalisation Using Social Media – Guidance for schools on how terrorist groups use social media to encourage travel to Iraq and Syria www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Better Internet for Kids – www.betterinternetforkids.eu

Anti-Bullying Network – Cyber-Bullying information for teachers and other professionals who work with young people – www.antibullying.net/cyberbullyin1.htm

Chatdanger – www.chatdanger.com