JRCS
E-Safety policy

Senior Team Responsibility:	Garry Smith Assistant headteacher
E-safety Co-ordinator:	Ciaran Sturdy Head of Computing
Date Reviewed:	February 2015
Next Review Date:	February 2016

1. Introduction

1.1 Jo Richardson Community School recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.2 As part of our commitment to learning and achievement we at Jo Richardson Community School want to ensure that the Internet and other digital technologies are used to:

- Raise educational standards and promote student achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable students to gain access to a wide span of knowledge in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding.

To enable this to happen we have taken a whole school approach to E-safety as promoted by the Child Exploitation and Online Protection (CEOP) and guidance on compliance by the Local Education Authority.

1.3 Jo Richardson Community School is committed to ensuring that **all** its students will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the risks that exist so that they can take an active part in safeguarding children.

2. Scope of Policy

2.1 The policy applies to:

- all students;
- all teaching and support staff, school governors and volunteers;
- All aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

2.2 Jo Richardson Community School will ensure that the following elements are in place as part of its safeguarding responsibilities to students:

- a list of authorised persons who have various responsibilities for E-safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using the Internet and other digital technologies;
- adequate training for staff and volunteers;
- adequate supervision of students when using the Internet and digital technologies;
- education that is aimed at ensuring safe use of Internet and digital technologies;
- A reporting procedure for abuse and misuse. (see appendix A)

3.0 Managing Information Systems

3.1 Internet security

At JRCS we take internet security seriously. To ensure that all school staff and students are safe we:

- Ensure that the school ICT system security is up-to-date and compliant.
- Virus protection will be installed and continually monitored to ensure it is ‘up to date’.

3.2 Email

- All students and staff have active email accounts which are regularly monitored by the network manager.
- Students are also taught email protocols during ICT lessons throughout the year; they are shown and told how to do this in year 7. During the e-safety module in year 7, 8 and 9 lessons 1-4. Key stage 4 students have a more focused and robust module on email.
- Students may only use e-mail accounts approved by the school on the internal systems, and they must immediately tell an appropriate member of staff if they receive offensive e-mail.
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Staff should only use their school email in communication with students and parents and are told this within the school handbook, and this is reinforced by the head teacher during staff briefings, reinforced by emails from the headteacher.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Students should be educated on how to deal with junk e mail and attachments.

3.2 Published content (network or on line)

- Staff or student personal contact information should not be published. The contact details given online should be the school office.
- The Headteacher has overall accountability and should ensure that published content is accurate and appropriate.

3.3 Publishing students’ images and work

- Parents / guardians sign the digital media release form to give their consent before photographs are used and do so when students start the school in September.

3.4 Social networking and personal publishing

- The school will control access to social networking sites, and ensure students are educated in their safe use. This is done with control and support of the Network Manager.
- Newsgroups, forums and chat-rooms will be blocked unless a specific use is identified and approved.
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location. This is done during lessons 1-4 at KS3 in years 7, 8 and 9; and then reinforced throughout the year through assemblies and the tutor time programme. At KS4 students take part in a Flash Based Animation project based on the dangers of social networking and e-safety.
- Students should not place personal photos on any social network space without

considering how the photo could be used now or in the future. This is covered in the safety lessons at KS3 and in the JRCS assembly

- Students should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others. This is done in by reinforcement by the ICT teacher, and the Network Manager whereby students are automatically told to change their password. This is done every half term by the ICT teacher via ICT lessons, and reinforcements within the school newsletter.
- All users (staff and students) are provided with a username and password by Network manager. All users (staff and students) are encouraged to change their password every half term. The following rules apply to the use of passwords:
    1. Passwords must be changed every half term
    2. The password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special character

3.5 Managing filtering

- The school will work in partnership with LBBD, and the Internet Service Provider to ensure that systems to protect students are reviewed and improved.
- If staff or students discover an inappropriate site, it must be reported to a member of staff who will pass it to the network manager, head of year or the child protection coordinator, depending on the nature of the site. In all instances the site will be blocked by the network manager

3.6 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and risks considered before use in school is allowed.
- The school is aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- The use of mobile technologies during school time is at the discretion of the Headteacher and governing body and at JRCS, mobiles are allowed before and after school and during break times. The sending of abusive or inappropriate data is forbidden and will result in confiscation of the mobile device.
- The school is ware that games stations of all varieties which have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- Staff should have access to a school phone where contact with students is required.

3.7 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and any other relevant legislation.

4.0 Policy Decisions

4.1 Authorising Internet access

All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.

- This is done at login via an automated programme script whereby all students have to accept the AUP to access the school network.
- The school will maintain a current record of all staff and students who are granted access to school ICT systems. This is kept by the Network Manager in the ICT office.
- Parents/carers will be asked to sign and return a consent form during the year 7 induction period.
- Staff complete an annual AUP, and this is kept by the schools administrative team.

4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor LBBD can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff in line with school policy.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- See also Appendix A

2.5 Communicating e-Safety

2.5.1 Introducing the e-safety policy to students

- E-Safety rules will be posted in all rooms where computers are used.
- Students will be informed that network and Internet use will be monitored.
- A programme of training in e-Safety will be developed, and based on the materials from CEOP, and current compliance thinking from the government and LEA.
- Students at the start of each year at Key Stage 3 in ICT complete a module on e-safety and cyber-bullying.
- Assembly programme also covers key aspects of communication with e-safety along with the schools newsletter.

2.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.

- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues. (see appendix A)
- Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.
- Staff must follow usual child protection procedures should the feel that aspect of e-safety has affected a member of students or staff well being.

2.6 Further information

The JRCS school website provides specific advice for staff/ students/ parents

- http://www.ceop.police.uk/safety-centre/
- http://www.thinkuknow.co.uk/
- http://jorichardson.publishpath.com/advice-on-cyberbullying
- http://jorichardson.publishpath.com/advice-for-parents--students
- http://jorichardson.publishpath.com/report-abuse
- http://jorichardson.publishpath.com/report-abuse

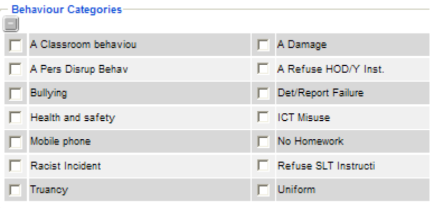
Appendix A

Procedure for reporting misuse of ICT

1. Member of staff defines the type of misuse of ICT

Type of ICT misuse	Level	Sanction
Accidental and non-malicious		
Accidental damage of ICT equipment	1	2 weeks limited ICT access
Printing abuse (accidental)	1	
Email abuse (inappropriate, immature, but not offensive)	1	
Internet abuse (inappropriate, immature, but not offensive)	1	
Intentional misuse		
Wilful damage of ICT equipment	2	1/2 term limited ICT access/ followed by CFC letter home
Printing abuse (wilful)	2	
Breach of another students login and password	2	
Email abuse (inappropriate and offensive)	2	
Internet abuse (inappropriate and offensive)	2	
Other (please state _____________)		All incidents of heightened concern should also be followed up through a brief CP referral.

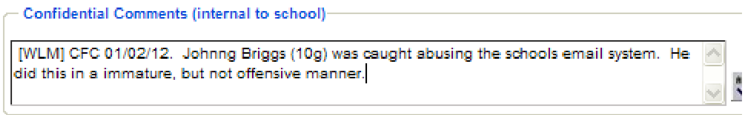
2. Member of staff creates a CFC and under the behaviour heading selects ICT misuse.



Behaviour Categories

□ A Classroom behaviou	□ A Damage
□ A Pers Disrup Behav	□ A Refuse HOD/Y Inst.
□ Bullying	□ Det/Report Failure
□ Health and safety	□ ICT Misuse
□ Mobile phone	□ No Homework
□ Racist Incident	□ Refuse SLT Instructi
□ Truancy	□ Uniform

3. Member of staff then in the confidential comments box defines the type of ICT misuse and then refers to either HOD/ HOY.



Confidential Comments (internal to school)

[WLM] CFC 01/02/12. Johnng Briggs (10g) was caught abusing the schools email system. He did this in a immature, but not offensive manner.

4. The HOD/ HOY will then inform the network manager of the type of ICT misuse and sanction, and the network manager will keep a record of the ICT misuse.

5. The network manager will only reinstate the ICT provision once he or she has had their planner signed by the member of staff who made the original referral.

As a good practice measure staff should always use the computer monitoring software provided to help safe-guard student's internet and email use

Appendix B

Parents' and Carers' guide to the Internet & e-safety

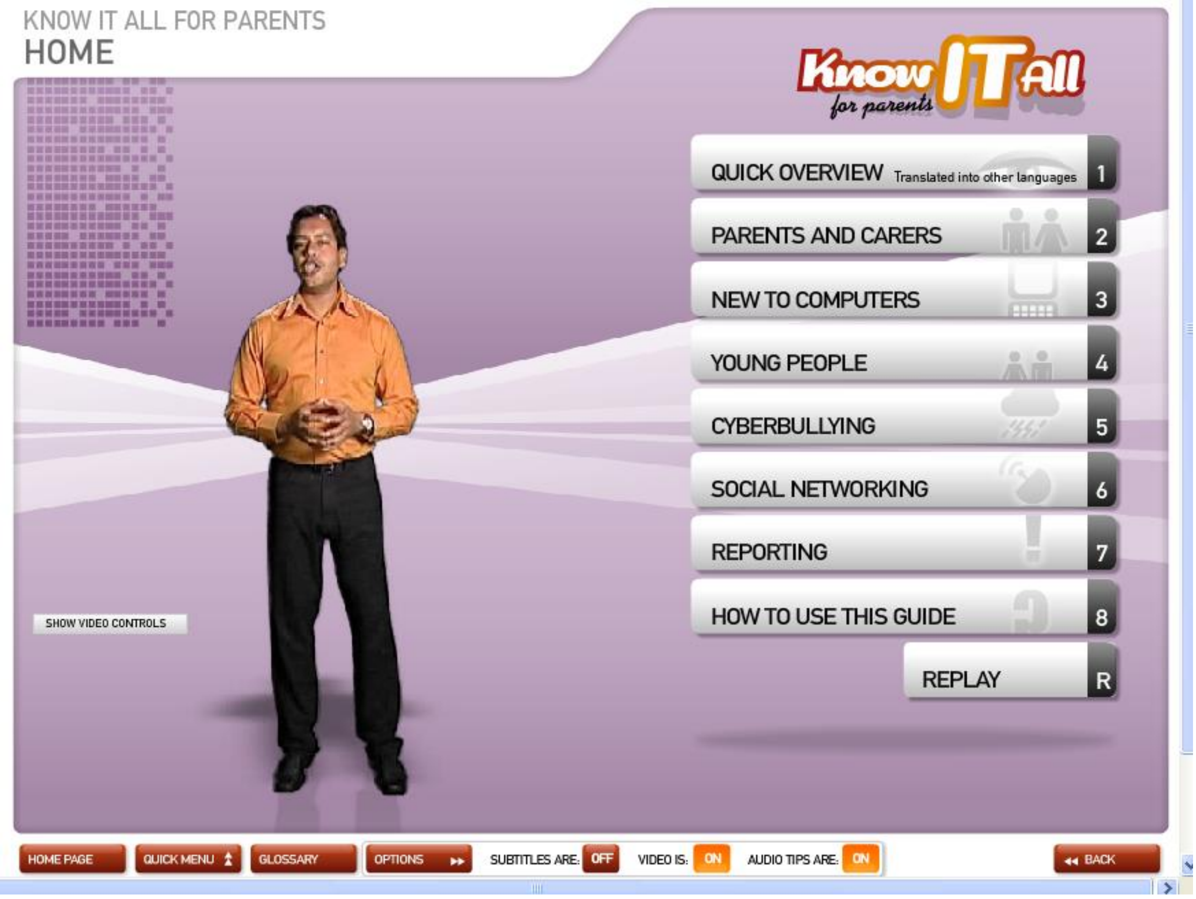
http://www.thinkuknow.co.uk/parents

1. **Be involved in your child's online life.** For many of today's young people there is no line between the online and offline worlds. Young people use the internet to socialise and grow and, just as you guide and support them offline, you should be there for them online too. Talk to them about what they're doing, if they know you understand they are more likely to approach you if they need support.
2. **Watch Thinkuknow films to learn more.** The Thinkuknow website (above) films and advice for children from five all the way to 16. Your child may have seen these at school, but they can also be a good tool for you to find out more about what young people do online and some of the potential risks.
3. **Keep up-to-date with your child's development online.** Be inquisitive and interested in the new gadgets and sites that your child is using. It's important that as your child learns more, so do you.
4. **Set boundaries in the online world just as you would in the real world.** Think about what they might see, what they share, who they talk to and how long they spend online. It is important to continue to discuss boundaries so that they evolve as your child's use of technology does.
5. **Know what connects to the internet and how.** Nowadays even the TV connects to the internet. Your child will use all sorts of devices and gadgets; make sure you're aware of which ones can connect to the internet, such as their phone or games console. Also, find out how they are accessing the internet – is it your connection or a neighbour's Wifi? This will affect whether your safety settings are being applied.
6. **Consider the use of parental controls on devices that link to the internet, such as the TV, laptops, computers, games consoles and mobile phones.** Parental controls are not just about locking and blocking, they are a tool to help you set appropriate boundaries as your child grows and develops. They are not the answer to your child's online safety, but they are a good start and are not as difficult to install as you might think. Service providers are working hard to make them simple, effective and user friendly.
7. **Emphasise that not everyone is who they say they are.** Make sure your child knows never to meet up with someone they only know online. People might not always be who they say they are. Make sure your child understands that they should never meet up with anyone they only know online without taking a trusted adult with them.
8. **Know what to do if something goes wrong.** Just as in the offline world, you want to help your child when they need it. Therefore, it is important to know when and how to report any problem. If you have a child who is in, or is due to start, primary school, read our primary school advice to find out what you can do to support them.

Top Tips

Open the excellent website below and play the excellent interactive resource below:

http://www.childnet-int.org.uk/kia/parents/cd/



SUBTITLES ARE: OFF

VIDEO IS: ON

AUDIO TIPS ARE: ON

Appendix C

Feel safe, be e-safe

"E-safety 10 Top Tips" for Children and Young People

1. Treat your password like your toothbrush – keep it to yourself!

2. Only give your mobile number or personal website address to trusted friends.

3. Block the bully – learn to block or report someone who is behaving badly.

4. Save the evidence – learn how to keep records of offending text messages, pictures or online conversations.

5. Don't retaliate or reply.

6. Check your profile and make sure it doesn't include any personal information.

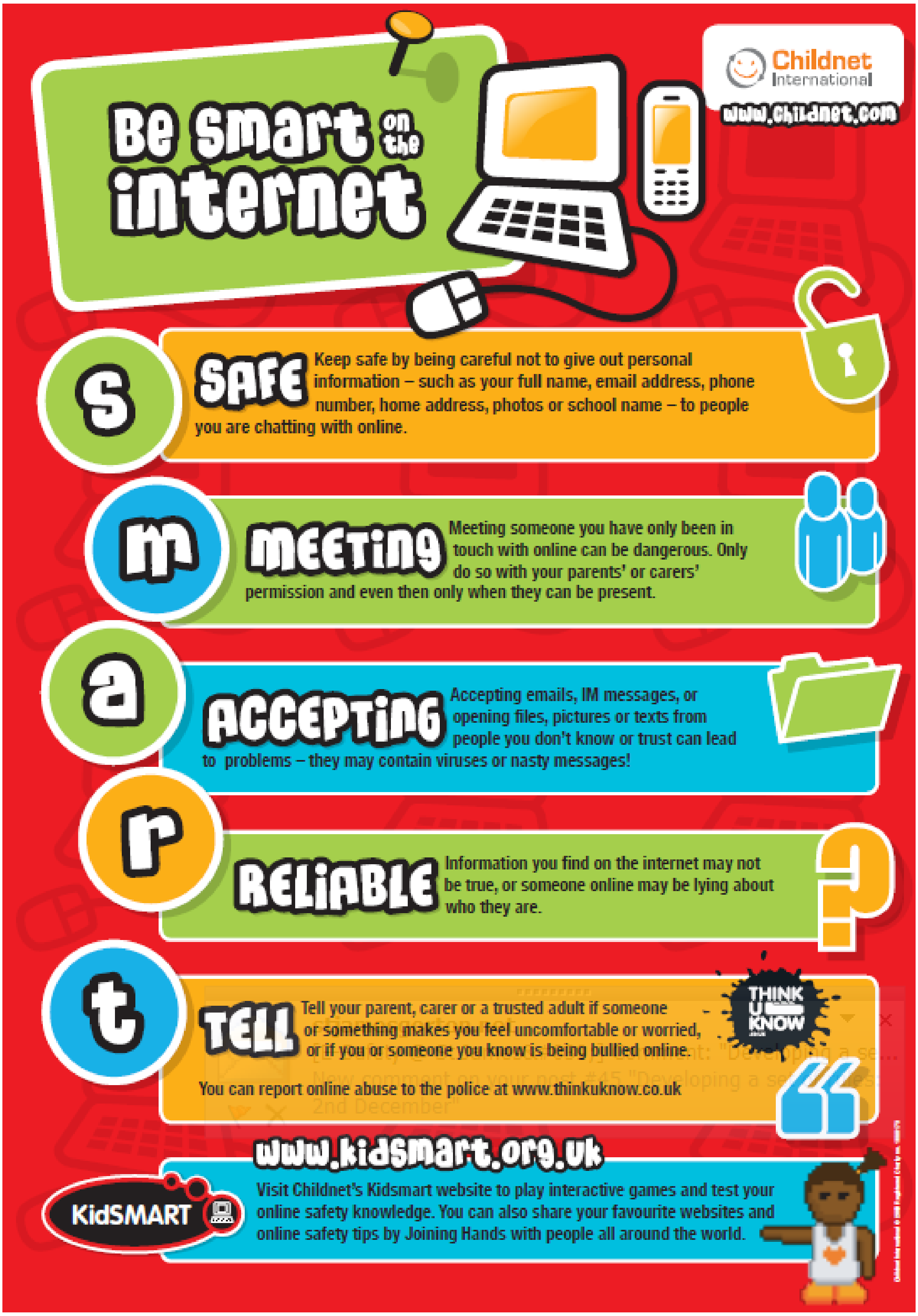
7. Always respect others – be careful what you say online and what images you send.

8. Think before you send – whatever you send can be made public very quickly and could stay online forever.

9. Look out for your friends – and do something if you think they are at risk.

10. Tell your parent, carer or a teacher if something or someone makes you feel uncomfortable or worried.

Finally, if you have other questions, contact www.thinkuknow.com or http://www.chatdanger.com for further information.



Be Smart on the internet

Childnet International
www.childnet.com

s SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

m MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

a ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

r RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

t TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Appendix D

Protecting staff: “simple dos and don’ts”

How to Stay ‘Cybersafe’ – Dos and Don’ts

Do

- be aware of your on-line reputation, which consists of information you post about yourself and information posted by others, and consider that when seeking employment, many prospective employers will use publicly available on-line information. Remember, the internet never forgets!;

- keep passwords secret and protect access to accounts;

- regularly review your privacy settings;

- discuss expectations with friends – are you happy to be tagged in photos?;

- be aware that, increasingly, individuals are being held to account in the courts for the things they say on social networking sites;

- keep personal phone numbers private and don’t use your own mobile phones to contact students or parents;

- ensure that school rules regarding the use of technologies are consistently enforced;

- report any incident to the appropriate member of staff in a timely manner;

- keep any evidence of an incident, for example by not deleting text messages or e-mails and by taking a screen capture of material, including the URL or web address.

- use school e-mail address only for work purposes.

- be aware that if you access any personal web-based e-mail accounts via the school network, that these may be subject to the school’s internet protocol which could include monitoring and surveillance.

- raise genuine concerns about your school or certain members of staff using your employer’s whistle blowing or grievance procedure.

Don't

- post information and photos about yourself, or school-related matters, publicly that you wouldn't want employers, colleagues, students or parents to see;
- befriend students or other members of the school community on social networking sites. (You should consider carefully the implications of befriending parents or ex-students and let school management know if you decide to do this.);
- personally retaliate to any incident, bullying messages;
- criticise your school, students or students' parents online.

More helpful tips are available from the UK Safer Internet Centre at www.saferinternet.org.uk under 'Advice and Resources'.

Or ask a member of the senior team