

Pupil E-safety & Acceptable Use Policy



This policy sets out Moorlands Primary School Pupil E-safety and acceptable use Policy and procedures.

Signed by Head Teacher _____

Signed by Chair of Governors _____

Review Date _____



Moorlands Primary School
Pupil E-safety and Acceptable Use

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Moorlands Primary School will ensure that this e-safety policy and accompanying guidelines supports the children in understanding that:

- The internet and digital communications are important
- Internet use will enhance learning
- It is important to evaluate internet content

Staff and pupils at the schools will not use social networking sites in school or on school owned devices.

The school's designated e-safety co-ordinator is: **Miss Sarah Roughton**.

Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught the importance of cross-checking information before accepting its accuracy. Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon.

1. E-Safety Risks & Issues

E-Safety risks and issues can be roughly classified into three areas: content, contact and commerce. The following are basic examples of the types of e-safety risks and issues that could fall under each category.

Content:

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse
- Downloading of copyrighted materials, e.g. music and films
- Plagiarism



Contact:

- Grooming using ICT, leading to sexual assault and/or child prostitution
- Bullies using ICT (email, mobile phones, chat rooms etc) as a way to torment their victims
- Children and young people self-publishing information - sometimes inappropriate - about themselves and therefore putting themselves at risk

Commerce:

- Exposure to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

2. Managing Filtering

All Moorlands Primary School, staff will work with Southampton County Council to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3. Roles and responsibilities:**Teacher responsibilities:**

The teachers are responsible for ensuring that:

- They establish and maintain a safe ICT learning environment within the school.
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable ICT Use Policy
- they report any suspected misuse or problem to their Phase Leaders
- digital communications with students / pupils should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupil responsibilities:

The pupils are responsible for:

- using the school ICT systems in accordance with the Student / Pupil Acceptable Use agreed rules “think then click”



- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
 - understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
 - Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
 - Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school.
 - Communicating with their parents or carers about internet safety issues, and upholding any rules for safe internet use in the home.
 - Ensuring that they abide by the school rules regarding appropriate websites and avoiding those banned e.g. YouTube and Facebook.
- **Parent and carer responsibilities**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Student / Pupil Acceptable ICT Use Policy "Think then click"
- Accessing the school website in accordance with the relevant school Acceptable ICT Use Policy.

4. Internet safety in the classroom

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access. E-safety rules will be located next to digital equipment and discussed with the pupils at the start of each year.
- Children are made aware of popular websites that they are not allowed to go in school, for example social media and Youtube. Staff may make use of Youtube / TeacherTube to support specific learning objectives on occasion, but this will not include children accessing it directly due to the ability to bypass filters on this site.
- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Through direct and discrete teaching, the children will be informed of the following:

- That network and Internet use will be monitored
- Keeping safe on the internet through the access of appropriate sites and activities.
- Who to inform should inappropriate material be viewed on a school computer



- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Copyright and infringement rules in accordance with the law to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

5. Social networking and personal publishing

The school will block/filter access to social networking sites.

- E-groups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices where possible.
- When personal data is stored on any portable computer system, USB stick or any other removable media (personal information relevant to children e.g. reports, IEP's etc)
 - the data should be encrypted and password protected if possible
 - the device must offer approved virus and malware checking software
 - the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

6. Incidents of misuse

- In the first instance, any inappropriate incident or account of Internet misuse should be reported to the Phase Leaders as appropriate.
- A log of inappropriate misuse must be made as close to the time of the relevant incident as possible and recorded on CPoms by the e-safety co-ordinator or other member of SLT and follow up accordingly.
- Phase Leaders will inform the head teacher and Senior Leadership Team accordingly. Liaising with ICT support /LA will also take place, if necessary, to ensure appropriate filtration and removal of any damaging / offensive material or potential viruses.



Internet misuse includes the following:

- Inappropriate materials or images viewed on the internet when filtered
- Accidental or deliberate attempts to view inappropriate material
- Any sites/ images linked to adult content, child abuse, racist materials etc
- Copyright infringement from information found on the internet
- Misconduct associated with student logins, such as using someone else's password
- Cyber-bullying in any context
- Allegations made against members of staff

7. Internet Code of Conduct

Pupils should be supervised at all times when using the Internet.

- Independent pupil use of telecommunications and electronic information resources is not permitted in school.
- Access to school systems must be with a unique user name and password, which must not be made available to any other staff member or pupil.
- All Internet activity should be appropriate to staff's professional activity or the student's education.
- Internet activity that threatens the integrity or security of the school's ICT systems, or activity that attacks, corrupts, or threatens the security of other organisations' systems, is prohibited.
- Copyrights, software licensing rules, laws of the land, property rights, privacy and the rights of others must be respected and adhered to at all times.
- The Internet must not be used to access, display, store, transmit, distribute, edit or record inappropriate sites such as those containing pornographic, violent, racist, discriminatory, criminal skills related, illegal drugs related or offensive material. Users will recognise materials that are inappropriate and, if deliberately accessing them, should expect to have their access removed.
- The Internet must not be used to download entertainment software or games, or play games against other Internet users.
- The Internet must not be used to conduct or host any on-going non-education related activities, including discussion groups, chat lines, newsgroups or any other form of on-line club.
- To ensure compliance with the acceptable use policy for Web browsing and email the school reserves the right to monitor and record activity in these areas. All users should therefore have no expectation of privacy in respect of their web browsing and email activities when using the school's computer facilities.

8. Email Code of Conduct

- Access to email should only be via the authorised user name and password, which must not be made available to any other staff member or pupil.
- Pupils may only use approved e-mail accounts on the school system.



- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Attachments from unknown sources should not be opened, but deleted immediately. All attachments should be scanned for viruses.
- Schools are responsible for all email sent and for contacts made that may result in email being received.
- Pupils must not send or publish their personal details in an email to an unknown recipient
- Posting anonymous messages and creating or forwarding chain letters is forbidden.
- As emails can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Messages that contain abusive or objectionable language, that libel others, or that infringe the privacy rights of others are forbidden.
- Changes must not be made to other people's messages that are then sent on to others without making it clear where the changes have been made.
- Users must not pretend that they are someone else when sending email, or use someone else's account to send a message.
- Users must not publish, electronically or otherwise, any school email address as a point of contact for non-education related activities.
- Personal or otherwise sensitive data must not be transferred via email unless the security of the data whilst in transit can be assured.

9. Social Networks, Chat Rooms, Instant and Text Messaging Code of Conduct

The school will control access to social networking sites, and consider how to educate pupils in their safe use. Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. Ideally pupils would use only moderated social networking sites. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils and some require the child to be at least 13 years of age. Pupils will be advised to use nicknames and avatars when using social networking sites.

- Pupils should only be given access to secure, age-appropriate chat rooms and social networks, which are moderated by a teacher, or recognisable, identifiable and approved adult.
- The use of such websites should only be permitted within an educational or professional context.



- Teachers should familiarise themselves with any chat room being used, to ensure that it offers a genuine educational experience.
- Pupils should be supervised at all times when using such websites.
- Pupils should be taught to understand the importance of personal safety on the Internet, i.e. taught never to give out personal contact information or to arrange to meet someone they have met online.
- Access to internet related services such as instant messaging, chat services and social networks is commonplace outside of the school environment. Many young people own, or have access to a mobile phone which provides online access. For this reason, schools will need to ensure that pupils are taught safe and responsible behaviours whenever using ICT while at the same time not promoting the use of certain sites, particularly where the minimum age for use is 13 years old.

10. Published content and the School Website Code of Conduct

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The school website will be accessed via a home page provided by the City Council, using the domain name www.moorlandsprimary.com
- The production and publication of any unofficial websites is strictly forbidden and, if undertaken will be actively pursued by the City Council for removal on behalf of the schools.
- A hyperlink will link the official home page to the school website, whether it is hosted with the City Council or externally.
- Only the designated staff member(s) within the school may upload material to the school website and all material for the website must be monitored and approved by the person(s) responsible. At Moorlands Primary School this named designated person is Miss Gemma Waring with the HT and SLT having overall editorial responsibility. The user name and password must not be given to any other members of staff or pupils. If other people know this information, the school will change the appropriate passwords.
- Images of pupils and staff should be classed as personal data under the terms of the Data Protection Act 1998. Therefore using such images for school publicity purposes, i.e. school web site will require the consent of either the individual concerned or in the case of pupils, their legal guardians.
- Recognisable photographs, full names, addresses, telephone numbers and email addresses of pupils must not be published on the school website. Home addresses and telephone numbers of school staff, parents and governors should not be published on the school website, where possible the school details should be given as the main point of contact.



- Southampton City Council reserves the right to remove any material from school websites if it is considered to be unsuitable or if it poses a threat to the safety of a school or pupil. Individual support and guidance on developing a school websites is available from CSL ICT Strategy telephone 023 8083 2111 or email csl.ict@southampton.gov.uk

11. Publishing Pupil's Images and Work Code of Conduct

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Where possible we will consider using group photographs rather than full-face photos of individual children.
- Pupil's full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs or published newsletters.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories
- The school will only enter work based competitions with not for profit organisations and only then after checks have been made and parents have signed to give permission for work to be submitted. The contact for the child will be the school's address not the child's own home address.

12. Managing Videoconferencing & Webcam Use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

13. Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The senior leadership team should note 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.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is



forbidden. Mobile phones are not permitted in school at KS1 for any reason. Please refer to Acceptable use of Mobile Phones at Moorlands Primary School for KS2 (**Appendix C**)

- The use by pupils of cameras in mobile phones is not permitted during or after school time. No pictures should be taken of staff or other children at after school events organised by the school or the 'Friends Association', such as discos and 'Friends' events. The school will investigate any reported cases of photos of staff or other pupils at such events being uploaded to social networking sites.

13. Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

14. Communications Policy

Introducing the e-safety policy to pupils

- All pupils and parents must read and sign the 'Moorlands E-safety contract' (**See Appendix D**) before using any school ICT resource.
- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- E-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website.
- The school will promote and provide links to a list of e-safety resources for parents/carers
- The school will ask all new parents to sign the 'Moorlands E-safety Contract' when they register their child with the school. (**see Appendix D**)

15. Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.

16. 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 SCC 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.



17. Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the headteacher, who may then consult LADO or HR. Complaints of a child protection nature must be dealt with in accordance with Moorlands Primary School child protection procedures. Pupils and parents will be informed of the complaints procedure (see schools complaints policy). Pupils and parents will be informed of consequences for pupils misusing the Internet.

Appendices

- A: Think then Click- Class use KS1
- B: Think then Click- Class use KS2
- C: Acceptable use of Mobile Phones (KS2)
- D: Moorlands E-Safety Contract
- E: Incident flowchart

This policy is to be read in conjunction with:

- Child Protection Policy
- Whistleblowing Policy
- Anti-bullying Policy
- Behaviour Policy
- Complaints Policy

This policy has been written using the guidelines provided by Kent Schools Core e-Safety Policy and Audit and Government Guidance 'Keeping Children Safe in Education' (September 2016)





Think then Click



These rules help us to stay safe on the Internet



We only use the internet when an adult is with us



We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.



We always ask if we get lost on the Internet.



We can send and open emails together.



We can write polite and friendly emails to people that we know.



Think then Click



E-Safety Rules for Key Stage 2

- **We ask permission before using the Internet.**
- **We only use websites that an adult has chosen.**
- **We tell an adult if we see anything we are uncomfortable with.**
- **We immediately close any webpage we are not sure about.**
- **We only e-mail people an adult has approved.**
- **We send e-mails that are polite and friendly.**
- **We never give out personal information or passwords.**
- **We never arrange to meet anyone we don't know.**
- **We do not open e-mails sent by anyone we don't know.**
- **We do not use Internet chat rooms.**



Moorlands Primary School

Parent and Pupil Emergency Mobile Phone Agreement



Your Child's Name _____ Class _____

Your name _____

Please explain why your child needs to have a mobile phone on them when they arrive/ leave school.

Mobile phone protocols

- * KS2 Parents will need to briefly explain why their child needs to have their mobile phone on them.
- * The phone is to be used for emergency use only on the journey to or from school.
- * The phone must not be used by the child on school premises.
- * Phones must be handed in to the class teacher as soon as the child arrives at school.
- * The phone must be clearly labelled with the child's name and class.
- * The child is responsible for collecting the phone. Any phones not collected will be locked away at the end of the day.
- * Parents take full responsibility for the phone and their child's use of the phone during the journey to and from school.
- * The school will take no responsibility for the loss of any phone.
- * Parents will be contacted if a child does not follow the agreement

Our policy is still that no mobile phones should be taken on residential/ day trips organised by the school in school time.

We understand and agree with all the protocols above and that failure to keep any part of the agreement may result in a complete mobile phone ban.

I have discussed the mobile phone agreement with my child and will support the school in implementing it.

Signed by parent _____ Date _____



I agree to follow the mobile phone agreement and have discussed how I will use my mobile phone with my parent.

Signed by pupil _____ Date _____

This agreement is in force until the end of July each year or sooner at the discretion of the school.



Appendix D

	<p>Moorlands Primary School E-Safety Rules</p>	
<p>All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the E-Safety Rules have been understood and agreed.</p>		
<p>Pupil:</p>		<p>Class:</p>
<p>Pupil's Agreement:</p> <ul style="list-style-type: none"> ✓ I have read and I understand the school e-Safety Rules. ✓ I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times. ✓ I know that network and Internet access may be monitored. 		
<p>Signed:</p>		<p>Date:</p>
<p>Parent's Consent for Web Publication of Work and Photographs</p> <ul style="list-style-type: none"> ✓ I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names. <p>Parent's Consent for Internet Access</p> <ul style="list-style-type: none"> ✓ I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. ✓ I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. 		
<p>Signed:</p>		<p>Date:</p>
<p>Please print name:</p>		
<p>Please complete, sign and return to school.</p>		



Appendix E

Moorlands Primary School

E-safety flowchart for incidents or misuse of the internet.
A guide for Phase Leaders, Head Teacher and SLT

Phase Leaders and / or Headteacher should:

- Record in the school E-Safety Incident Log
- Keep any evidence

If member of staff has:

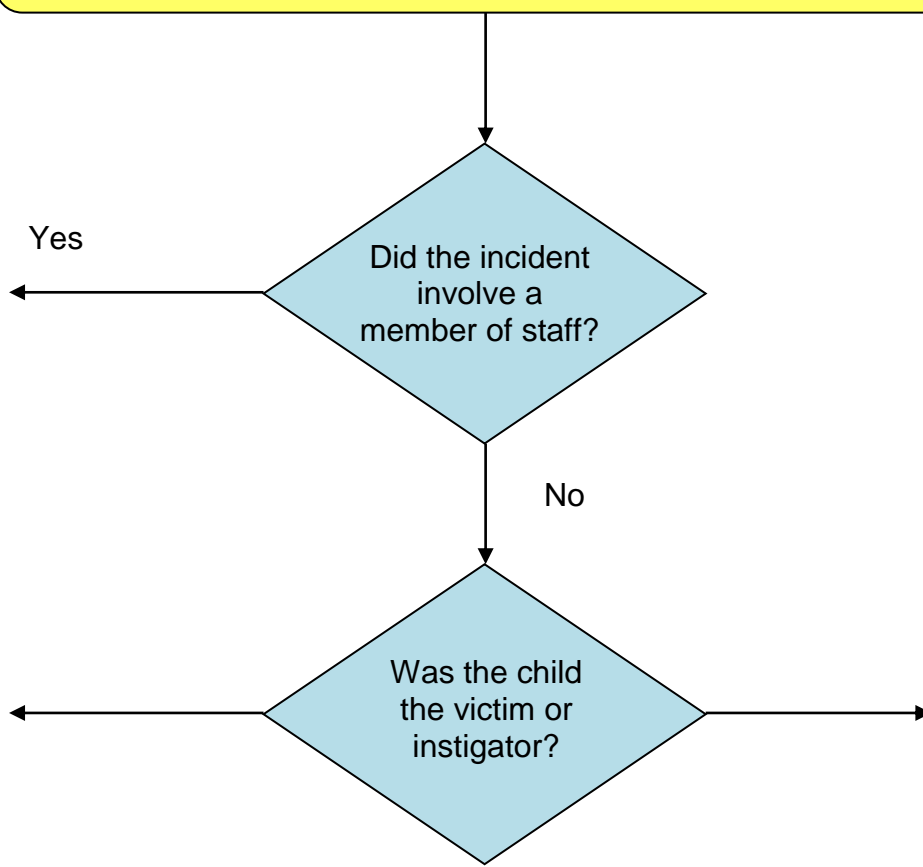
1. Behaved in a way that has, or may have harmed a child.
2. Possibly committed a criminal offence.
3. Behaved towards a child in a way which indicates s/he is unsuitable to work with children.

- Review evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate) and contact school HR

In –school action to support pupil by one or more of the following:

- Class teacher
- Phase Leaders
- Senior Leader or Headteacher
- Child Protection officer (CPLO)
- Inform parents/ carer as appropriate
- Confiscate the device, if appropriate.

If the child is at risk inform CPLO immediately



If the incident **did not** involve **any illegal activity** then follow this flowchart

Incidents could be:

- Using another person's user name and password
- Accessing websites which are against school policy e.g. inappropriate materials
- Using the technology to upset or bully (in extreme cases could be illegal)

Users must know to **switch off their monitor or close laptop** if they find something unpleasant or frightening and talk to a member of staff or phase leaders

