



**St Mary's Voluntary Catholic Primary
Academy**

ICT Online safety and acceptable use policy

Introduction:

The purpose of this policy is to ensure that all users of all forms of ICT, understand the way in which these resources are to be used; with specific reference to Internet & e-mail use. The policy also aims to ensure that the Internet is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risks. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. This contributes to development of the key area of developing pupils' life skills to enable future economic well-being.

ICT & Internet access in school is there to raise educational standards, to support the professional work of staff and to enhance the school's information management and business administrative systems. ICT & Internet access is a necessary part of the statutory curriculum. The Early Years Foundation Stage and the National Curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT (Information and Communications Technology). Within the curriculum, teachers need to plan for, and make use of, communications technology, for example, web-based resources and email. Access to life-long learning and employment increasingly requires computer and communications use and pupils need to develop the associated skills. Of paramount importance is the protection of the children. Every activity is designed to minimise any risk to the children, while enhancing their education. **Internet use is an entitlement for pupils based on responsible & acceptable use (refer to 'pupil roles and responsibilities').**

Users should read this policy alongside the school's ICT Policy.

Aims:

- To provide full protection for the school community.
- To raise educational standards through accessing global educational resources.
- To support the professional work of staff through access to educational materials and good curriculum practice.
- To enhance the school's management, information and administration systems. To protect users in school through using a filtered system.
- To protect all children from exposure to inappropriate use of children's photographs on the web.

Roles and responsibilities

All users of ICT within the school and the wider community are to be made aware of their own roles and responsibilities, to ensure internet safety and to minimise online safety risks. All adults and children must adhere to their responsibilities.

- The school has appointed an online safety co-ordinator (Mrs Phelps) who will manage and monitor online safety.
- The technician regularly monitors internet access and brings any issues to the attention of the online safety co-ordinator who then takes appropriate action.

The school has clearly set out roles and responsibilities in relation to internet use and these can be seen in the Appendix.

Internet Usage:

Teachers, parents and pupils need to develop good practice in using the Internet, as a tool for teaching and learning. Internet access will be planned to enrich and extend learning activities. Staff will select sites that will support the learning outcomes planned for pupils' age and maturity and set clear learning objectives for Internet use.

Benefits of use include:

- Access to approved world-wide educational resources
- Information and cultural exchanges between students world-wide via e-mail and video conferencing when appropriate
- Staff professional development – access to educational materials and good curriculum practice

St Mary's expects all users to use the Internet responsibly according to the rules and responsibilities document set out in the appendix.

Users shall not visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography
- promoting discrimination of any kind promoting racial or religious hatred promoting illegal acts
- any other information which may be offensive to colleagues, peers and the wider community.

It is acknowledged that in certain planned curricular activities access to sites, otherwise deemed inappropriate, may be beneficial for educational use (for example investigating racial issues). Any such access will be pre-planned and recorded so that it can be justified, if required.

Incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following material will be reported to the police:

- Images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative.
- Adult material that potentially breaches the Obscene Publications Act in the UK. Criminally racist material in the UK.

If any unsuitable material has slipped through the filtered system and is found by adults or children, it will be reported immediately to the head teacher who will inform the LA at and the Police if of an extremely serious nature. If an adult or pupil accesses an unsafe site the monitor should immediately be switched off, but the computer left on, so a note can be made of the web address. **All incidents will be reported in the Online safety Incident Report Book in the school office.**

Pupils and adults will be given clear guidelines when using the Internet and taught about safe use of the Internet. Internet access will be planned to enrich and extend learning. Teachers will select, and help children to select, websites appropriate for their age. The Internet will not replace books but will provide an additional learning resource for children. Children will be taught to assess which is the most appropriate resource to support learning objectives and ways to validate information before accepting that it is necessarily accurate. Safe use of the Internet for children (Acceptable use guidelines) will be displayed for pupils and adults in classrooms.

Parents will be informed of acceptable use guidelines in the new parent pack and when this policy is reviewed.

Chat rooms and newsgroups will not be used in school.

It is not permitted for anyone to use school computers for any form of illegal activity, for example downloading copyright materials, introducing viruses, etc.

Online safety scheme of work:

The school follows the CEOP and Think U Know schemes, which educate children to be aware when using ICT. It is the responsibility of each class teacher to ensure that all children are aware of their role as a responsible ICT user. The school also follows the Chris Quigley Essentials curriculum.

School Web-Site:

The school website is used to provide up-to-date news to parents and access to all relevant school documents. Both teaching and non-teaching staff are responsible for sending material to the website manager at e-limelight. All material posted on the website will comply with all rules regarding internet acceptable usage.

The school follows these guidelines to ensure children are not put at risk, by inclusion of photos on the website;

- o Parents may request photographs that include their child never to be entered onto the website.
- o Parents may request that a particular photo be removed or not included.
- o Full names of children will not be in any way associated with an image.
- o There will be no contact information other than for the school.

Use of Images

The school keeps up- to- date records of parental permission for the use of children's images. Photographs are taken using school digital cameras and ipads only. No photographs will be associated with children's names or personal details unless the parent has requested that the information be given eg. Sporting achievements.

Communication

All members of staff have secured school email addresses that are used for correspondence and file sharing.

Guidelines for staff email use:

- o Check e-mails regularly, reply to e-mails and keep a copy of incoming business related e-mails.
- o The school e-mail system should not be used by any user for the sending of personal mail unconnected with school work or activity.
- o Any e-mail received by a member of staff, which is regarded as illegal or offensive, should be reported to the Head teacher immediately.
- o To safeguard against computer viruses do not open external emails or an email attachment that look in any way suspicious. Report it to the school's ICT team for checking.
- o The school will e-mail any school letters/newsletters to parents if the e-mail address is provided by the parents.

Network, Laptop, Digital Camera, Projectors:

Staff using the school network, laptops, digital cameras, ipads, projectors or any other form of digital device or media, whether at school or off- site, must still abide by the agreed rules regarding the acceptable use of internet, e-mail & images.

Mobile Phones

The school policy is that pupils are not allowed mobile phones in school. The school phone can be used to contact parents/carers with important messages. Staff are not permitted to use their personal mobile phones to take images of the children.

Social networking and personal publishing

The school will filter access to open social networking sites and give access only to those sites that are monitored and approved by the Academy trust and Redcar and Cleveland. All communication will be treated as 'public' and children will be asked to agree and sign a code of conduct before access to these tools is given. Misuse of these tools will lead to the application of sanctions including prohibiting or limiting access.

Although pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils, pupils will be taught about the potential risks of social networking sites and what information should not be shared on such sites. The purpose of this is to acknowledge (although not condone) the reality that some children may already have access to social networking sites by this age. If it is discovered that children do have access to such sites a general letter will be sent to all parents advising of the sites regulations, however individual children will not be identified.

The School uses social media to communicate with parents and share achievements and interesting activities in and out of school. Parents are asked for consent to their child's image being used on the school Social Media sites. The site will also be used to share important information. It has been communicated to parents that use of the site is for information and all problems and issues should be raised in school not via this site.

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.

Conclusion

Access to the internet and digital communication media have the potential to greatly enhance learning and engagement with parents and our school is committed to extending these opportunities whilst maintaining the highest standards of safety. Everyone in school has a personal responsibility to work towards keeping themselves and others safe online.

Review

This policy will be reviewed by the Senior Management Team, Staff & ICT team on an annual basis and should be read in conjunction with the equal opportunities, inclusion and ICT policies.

January 2016

Signed..... Headteacher

Signed..... Chair of Governors

ICT ONLINE SAFETY AND ACCEPTABLE USE POLICY

Appendix 1 – Roles and responsibilities

Governors

Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The role of the Online safety Governor will include:

- regular meetings with the Online safety Co-ordinator / Officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Parents

Parents/carers should discuss use of the internet with their children and take the opportunity to reinforce the national messages being provided by the school. The text below gives some ideas for parents to use when discussing and monitoring internet use with young people. It has been written in language which is accessible by young people so that it can serve as a prompt for opening up discussions between parents/carers and young people about the main issues.

Home Use of the Internet

Parents / carers should:

- Ensure that children access the internet in a communal room where they can be easily supervised
- Ensure appropriate supervision for the age of their children including supervising all use of the internet by younger users
- Ask their children about what sites they are looking at
- Ensure that family computers are password protected and have robust anti-virus software which is regularly updated
- Ensure content is appropriately filtered for younger users

Head teacher and senior leaders

- Take a lead in embedding safe internet practices into the culture of the school.
- Ensure sufficient professional development time is allocated for information to be effectively disseminated and for colleagues to receive training if required
- Follow up any issues raised by the online safety co-ordinator
- Ensure that parents are kept up to date with issues relating to online safety

Online safety co-ordinator

- Central point of contact for all online safety issues Drafting policies and keeping them up to date
- Ensuring policies are adhered to
- Monitor breaches and abuses and report them to the head and governors
- Ensuring that all staff receive relevant information about emerging issues, this could include breaches by individuals
- Liaise with the ICT Subject Leader / Network Manager to ensure that technological solutions to online safety support classroom practice
- Identify any training issues for staff linked to acceptable use and bring

- o these to the attention of the head teacher / governors
- o Have an overview of where acceptable use is taught across the school

Teaching and support staff

- Ensure, when using ICT in the classroom, that they take regular opportunities to remind children about issues linked to online safety and discuss them
- Ensure that they are fully informed about the school online safety policy and ensure that pupils adhere to this at all times
- Bring any breaches of policy to the attention of the online safety co-ordinator
- Ensure that they model safe use of ICT and the internet including specific searches Ensure that they use resources appropriate to the age of the pupils they are working
- with
- Take up professional development opportunities to update their knowledge in this area and seek guidance when required
- Provide additional guidance, support and supervision for pupils with special educational needs where appropriate
- Be aware and comply with the school's policy on the use of Social Media **(See Appendix 4)**

In lessons where internet use is pre-planned children 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

Children

The children are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to read and agree to before being given access to school systems. Through carefully planned and structured schemes of work they should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

They will also be expected to:

- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- 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.
- understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy also applies to their actions out of school.

Appendix 2 – Pupil Acceptable Use and online safety Policy Agreement

Introduction

The purpose of this policy is to ensure that young learners know how to use the internet and other technologies responsibly and know what to do if they discover harmful content on the internet.

Finding information on the internet

I Know:

- that I will get to use the internet if I use it responsibly, and that being responsible means trying not to visit unsafe sites or registering for things I am not old enough for
- what to do if I open something I do not like how to search the internet safely
- that any information I put on the web can be read by anyone
that I should not copy others' work and use it as my own

Using technology to contact people

I know:

- how to protect my identity and keep my personal information private
how to use the safety features of websites
- that I should be careful who I add as friends
that I need to be polite and friendly online
- not to open e-mails if the subject is offensive or if I do not know who it is from
what to do if I receive an offensive e-mail/message
- that people online may not be who they say they are

Using technology for buying and selling

I know:

- how to tell the difference between websites for information and websites that sell things
- how to recognise the use of the internet for selling things (I Tunes, mobile phone downloads, shopping)
- That I should not use someone else's identity to buy things online

Signed _____ Date _____

Class Teacher _____

Appendix 3 – Guide for parents

Monitoring Home Use of the Internet

Parents / carers should:

- Ensure that young people access the internet in a communal room Ask their children about what sites they are looking at
- Ensure that family computers are password protected and have robust anti-virus software which is regularly updated
- Ensure content is appropriately filtered for younger users

Content – finding and publishing information on the internet

Parents / carers should:

- Ensure that their children know that they will only get to use the internet if they use it responsibly and that being responsible means they should not try to visit unsafe sites or register for things they are not old enough for.
- Ensure that their children know that any protection system does not stop all unsafe content and that children need to tell them if they access something inappropriate.
- Encourage children to search safely to find the information they want and search safely themselves using very specific search terms to reduce the likelihood of accessing unsafe material.
- Supervise younger children when they are using the internet.
- Talk to children about the fact that any information published on the web can be read by anyone.
- Check information that younger users are publishing on the web before it is posted to ensure that they are not putting themselves in danger.

Contact - Using technology to contact people

Parents / carers should:

- Discuss user names with children and talk about how to choose them carefully to avoid putting themselves at risk and protect their identity.
- Identify the information that young people should keep private in order to prevent them being contacted or traced including.
- Talk to children about the need to use safety features of web sites.
- Talk to their children about limiting access to their personal information.
- That e-mails / messages can be intercepted and forwarded on to anyone should talk to their children about being careful who they add as friends.
- Talk about the need to be polite online and friendly online and think about the language they use (it could be forwarded to my parents or head teacher!) Discuss how to use the subject field in e-mails.
- Not to open messages if the subject field contains anything offensive or if I do not recognise who it is from (delete it without opening it)
- Discuss what to do if I receive an offensive message / e-mail including how to keep evidence.
- Explain that people online may not be who they seem