St Wystan's School
E-safety policy

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment.

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At St Wystan's School we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, camera phones and portable media players, etc).

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 ICT co-ordinator has been designated the role of e-safety co-ordinator as part of the overall ICT co-ordinator role. All members of the school community have been made aware of who holds this post. It is the role of the ICT coordinator to keep abreast of current issues and guidance through organisations such as Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

The Head/ICT coordinator updates the SLT and Governors and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

E-Safety skills development for staff

- Staff receive information and training on e-Safety issues when relevant, through the coordinator at staff meetings.
- 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.
- New staff receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons, and we have an internet safety week every year to ensure all children are well informed.

E-Safety information for parents/carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- The school will send out relevant e-Safety information through newsletters and the school website.

Community use of the Internet

External organisations using the school's ICT facilities must adhere to the e-Safety policy.

Teaching and Learning

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach e-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the ICT curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP. Refer to the Anti-Bullying policy for more information.
- 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.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use.
- Pupils may be given a suitable web page or a single website to access.
- Pupils may be provided with lists of relevant and suitable websites which they may access
- Older, more experienced, pupils may be allowed to undertake their own internet search having agreed a search plan with their teacher.
- Pupils will be encouraged to use the 'Hector Protector' button to hide any material that they know is unsuitable for viewing. This will instantly cover the whole screen until it can be dealt with by the class teacher.
- Pupils are encouraged to immediately close the browser and inform a teacher when they come across unsuitable material.
- 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 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Parental Support

Parents may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Managing Internet Access

Information system security

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly using Microsoft Security Essentials.
- Security strategies will be discussed with the Headteacher and Governors.

E-mail

- Pupils may only use simulation e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.

Published content and the school web site

The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will **not** be published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The Head of Marketing will regularly update the school website.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are used in school marketing materials. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- 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 St Wystan's School Website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Photographs taken by parents/carers for personal use

On the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. School performances and assemblies etc.

Social networking and personal publishing

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are advised to never add or accept children as 'friends' if they use these sites.

Managing filtering

- The school will work with Unify and Netfactory and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If pupils or staff discovers an unsuitable site, it must be reported to the Class Teacher, ICT Coordinator or Headteacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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 use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.
- Pupils are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school will be sent to the school office and kept there until the end of the day.
- The sending of abusive or inappropriate text messages outside school is forbidden.
- Staff will use a school phone where contact with parents is required.
- Staff should not use personal mobile phones during designated teaching sessions, or within sight of parents/pupils/visitors.

Protecting personal data

The school will collect personal information about you fairly and will let you know how the school will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school. For other members of the community the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school.

The school will hold personal information on its systems for as long as you remain a member of the school community and remove it in the event of your leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, as defined by the Data Protection Act 1998.

You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

Policy Decisions

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's Think then Click e-Safety rules. These e-Safety rules will also be displayed clearly in all networked rooms.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.
- All staff must read and agree in writing to adhere to the Staff Code of Conduct for Staff before using any school ICT resource.

Password Security

- Adult users are provided with an individual network username and password, which they are encouraged to change periodically.
- All pupils are provided with a class username and password.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

Assessing risks

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. The school cannot accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.

Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the ICT coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT coordinator and recorded in personal files.
- 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.
- Pupils and parents will are informed of the complaints procedure.

Communications Policy

Introducing the e-Safety policy to pupils

- E-Safety 'Think and Click' rules will be displayed in all classrooms, the hall, music room and the ICT suite and discussed with the pupils at the start of each year.
- Pupil will only be allowed to use the internet once these rules have been taught.
- Specific lessons will be taught by ICT teachers at the beginning of every year and at relevant points throughout e.g. during PSHE lessons/circle times/anti-bullying week.
- Pupils will be informed that network and Internet use will be monitored**.**
- The 'Hector the Protector' e-safety button will be discussed and its use encouraged when inappropriate material is displayed.

Staff and the e-Safety policy

- All staff will be given the School e-Safety policy and its importance explained.
- Teaching and Support Staff are responsible for ensuring that they have an up to date awareness of online safety matters and of the current school e-Safety Policy and practices.
- They will have read, understood and signed the Staff Acceptable Use Agreement.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff are aware that they must report any suspected misuse to the Headteacher.
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- Staff will ensure that their pupils understand and follow the e-Safety 'Think and Click' rules and that these remain uppermost in the children's minds when using the internet.
- Staff monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Writing and reviewing the e-Safety policy

This policy, supported by the school's Acceptable Use Agreement for staff, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for ICT, Behaviour, Health and Safety, Child Protection, and PSHE policies including Anti-bullying.

Policy Development and Review

This document was produced in consultation with the school community, including pupils, parents, school staff and Governors.

This document is freely available to the entire school community. It has also been made available on the school web-site.