The Warriner School

Internet and Acceptable Use Protocol

The Warriner School's E-Safety, Internet and Acceptable Use protocol has been devised by the Senior Leadership Team and ICT Coordinator.

Introduction

The use of ICT including 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.

The purpose of ICT use in The Warriner School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

Core Principals of E-Safety Policy

E-safety encompasses ICT technologies and electronic communications such as mobile phones as well as collaborative tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's E-safety protocol will operate in conjunction with other policies and protocols including those for Behaviour, Bullying, Curriculum and Data Protection[1].

E-safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Local Authority (LA), as part of the Oxfordshire Communication Network.
- National Education Network standards and specifications.

The Warriner School's E-Safety, Internet and Acceptable Use protocol is built on the following core principles:

Teaching and learning

Significant educational benefits result from the use of ICT: including access to information from around the world and the abilities to communicate widely and to publish easily. ICT use should be planned, task orientated and educational within a regulated and managed environment.

[1] All related policies in this section are referenced as The Warriner School (2015)

Directed and successful ICT use will also reduce the opportunities for activities of dubious worth.

We operate a 'B4L' (Behaviour 4 Learning) policy in school. One of the specific categories on this list is 'Misuse of ICT'. Misuse of ICT results initially in a Formal lunchtime detention.

Benefits of using the Internet in education include:

- Access to world-wide educational resources
- Development of the Personalized Learning agenda e.g. though access to Oxfordshire's VLE – The Kaleidos Learning Platform (KLP)
- Access to experts in many fields for students and staff
- Staff professional development through access to national developments, educational materials and good curriculum practice, inclusion in government initiatives such as DCSF, NCSL, Teachernet, and local OCC training courses
- Communication with support services, professional associates and colleagues
- Exchange of curriculum and administration data with the LA and DCSF
- Mentoring of students and provide peer support for them and teachers

The School ICT facilities are designed expressly for student and staff use and includes user group specific filtering. Students are taught what ICT use is acceptable and what is not and given clear objectives for use.

In Year 7 students are issued with a booklet called the 'Network Guide' which covers our student acceptable use policy and also has the 'Rules for Responsible use of Computers in School'. (See appendix 1)

This is also sent out as a document with the admissions pack so that students and parents have signed and returned the agreement to school before they enter an ICT or Network room.

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become "ICT wise". We aim to ensure that students are fully aware of the risks, perform risk assessments and implement a policy for ICT use. Students need to know how to cope if they come across inappropriate and illegal material.

Using the ICT facilities

Internet

On turning on the schools computers the pre-login page displays the following message warning users that they are agreeing to abide by the Rules for responsible use of computers in school.
(See appendix 2)

If staff or students discover unsuitable sites with inappropriate pornographic content (containing only adults) the URL (address) and content should be recorded. Relevant

Leadership Team member or IT Manager should be informed immediately and given the details. They will take appropriate action which will include making contact with parents and limiting / discontinuing student e-access.

If staff or students discover unsuitable site with illegal content (containing adults and children) the computer should be immediately shut down, once the URL (address) and content have been recorded, and secured. The relevant Leadership Team member or IT Manager should be informed immediately and given the details. They will inform the Headteacher, the police and the LA. Contact with parents and limiting / discontinuing student e-access will be the minimum outcome.

Viewing of other inappropriate or illegal content will also lead to contact with parents being made and limiting / discontinuing student e-access.

The School will do all it reasonably can to ensure that the use of Internet derived materials by staff and by students complies with copyright law.

Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Email

- Students may only use appropriate Internet e-mail accounts on the school system
- Students must immediately tell a teacher / tutor / Director of House if they receive offensive email
- Staff must only use the school email system, not own personal e-mail address, to contact children / outside agencies / other schools / staff / Educational Establishments
- Staff and children's student email accounts may be monitored

Web Site

- Permission from parents or carers will be obtained before photographs of students are published on the school web site
- Students' full names will not be used anywhere on the web site, particularly in association with photographs
- The designated Leadership Team member (Nic Parry) will take overall editorial responsibility and ensure that content is accurate and appropriate
- The copyright of all materials must be held by the school, or be attributed to the owner where permission to reproduce has been obtained

Social Networking and Personal Publishing

- Students will not be allowed access to public or unregulated chat rooms
- Students should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised
- Users are not to use instant messenger types of programmes or chat rooms

- Students will be advised never to give out personal details of any kind which may identify them or their location

Managing Videoconferencing

- Videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet
- Videoconferencing must be supervised at all times

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998[2]

Management of emerging Internet Applications

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Other facilities & hardware generally

All users should treat the ICT equipment and facilities carefully and with respect to ensure that others can use them in the future.

Policy Decisions

Authorised ICT Access

The school will maintain a current record of all users who are granted access to school ICT systems.

Students and parents/carers will be asked to sign and return a consent form which is sent out as part of the admissions process.

Assessment of Risks

In common with other media, some e-material is unsuitable for students. 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 the Local authority can accept liability for the material accessed, or any consequences of Internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990[3].
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the E-safety and Internet protocol is implemented.

[2] Uk Government (1998) Data Protection Act as accessed via http://www.legislation.gov.uk/ukpga/1998/29/contents on November 22nd 2012

[3] UK Government (2000) Computer Misuse Act as accessed via http://www.legislation.gov.uk/ukpga/1990/18/contents on 22nd November 2012

E-safety depends on staff, schools, governors, advisers, parents and the students themselves taking responsibility for the use of Internet and other communication technologies. The balance between educating students to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied, for instance un-moderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help students make responsible decisions.

Handling e-safety complaints
Complaints of Internet misuse will be dealt with the relevant Senior Leadership Team member. Any complaint about staff misuse will be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Students and parents will be informed of the complaints procedure via the school website.

Communicating e-Safety
This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding students towards educational activities. Strategies must be selected to suit the school situation and their effectiveness monitored. There are no straightforward or totally effective solutions and staff, parents and the students themselves must remain vigilant.

- Parents' attention will be drawn to the School E-Safety and Internet Protocol in newsletters.
- The school will work in partnership with parents, the LA, and the ISP to ensure systems to protect students are reviewed and improved.
- Rules for e-safety will be posted in all rooms where computers are used and discussed with students at the start of each year.
- Students and staff will be informed that network and Internet use will be monitored.
- All staff must read and accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- The school will keep a record of all staff and students who are granted Internet access.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet protocol, and its importance explained.
- Staff should be aware that Internet traffic and inappropriate use of Internet facilities will be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will not use MSN Messenger or any other chat rooms.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.

- The school ICT systems will be reviewed annually with regard to security.
- Virus protection will be installed and updated regularly.
- Unapproved system utilities and executable files will not be allowed in work areas or attached to e-mail.
- Files held on the School's network will be regularly checked.
- Any complaint about staff misuse must be referred to the Headteacher.

Review
This protocol will be reviewed annually in line with the school's policy and protocol review programme.
The relevant Leadership Team member is responsible for reporting to governors about the quality of its implementation and its impact on standards.

Appendices
1. Students rules for responsible use of computers in school
2. Login Script
3. Internet Use at The Warriner School
4. Staff Information Systems Code of Conduct

Notes on the legal framework
The Computer Misuse Act 1990[4] makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data.

The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Contravention of Human Rights and Fundamental Freedoms[5], e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998[6]. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000[7] also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day to day activities.

[4] UK Government (2000) Computer Misuse Act as accessed via http://www.legislation.gov.uk/ukpga/1990/18/contents on 22nd November 2012
[5] European Convention on Human Rights (2010) as accessed via http://conventions.coe.int/treaty/en/treaties/html/005.htm on 22nd November 2012
[6] UK Government (1998) Human Rights Sct as accessed via http://www.legislation.gov.uk/ukpga/1998/42/contents on 22nd November 2012
[7] UK Government (2000) The Telecommunications (Lawful Practice) (Interception of Communications) Regulations as accessed via http://www.legislation.gov.uk/uksi/2000/2699/regulation/3/made on 22nd November 2012

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others.

Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place. Schools should start by banning private use of a school's computer system, but then allow private use following application to the Headteacher.

The Rules for Responsible use of Computers in School, which every student must agree to, contain a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring. The following legislation is also relevant:

Data Protection Act 1984[8]/98[9] concerns data on individual people held on computer files and its use and protection.

Copyright, Design and Patents Act 1988[10] makes it an offence to use unlicensed software.

The Telecommunications Act 1984[11] section 43 makes it an offence to send offensive or indecent materials over the public telecommunications system.

Protection of Children Act 2004[12]

Obscene Publications Act 1959[13] and 1964[14] defines 'obscene' and related offences.

Drafted: June 2015 By: Head of ICT

Next Review: Term 5/6 (2012-2013)

[8] UK Government (1984) The UK Data Protection Act as accessed via http://mcs.open.ac.uk/kgw9/interesting/dataprotection.htm on 22nd November 2012
[9] UK Government (1998) Data Protection Act as accessed via http://www.legislation.gov.uk/ukpga/1998/29/contents on 22nd November 2012
[10] UK Government (1988) Copyright, Design and Patents Act as accessed via http://www.legislation.gov.uk/ukpga/1988/48/contents on 22nd November 2012
[11] UK Government (1984) The Telecommunications Act as accessed via http://www.legislation.gov.uk/ukpga/1984/12 on 22nd November 2012
[12] Uk Government (1978) The Protection of Children Act as accessed via http://www.legislation.gov.uk/ukpga/1978/37 on 22nd November 2012
[13] UK Government (1959) Obscene Publications Act as accessed via http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents on 22nd November 2012
[14] UK Government (1964) Obscene Publications Act as accessed via http://www.legislation.gov.uk/ukpga/1964/74 on 22nd November 2012

Appendix 1 - Student rules for responsible ICT use

The Warriner School - Rules for responsible use of computers in school

Access to the school network is provided to aid learning. These rules are to keep the use of computers in school safe, and to help us to be fair to others.

By logging on to, and using, the school computer network I indicate that I understand and accept the following conditions:

- I will only log on to the system in the way that I have been shown using my own username and password.
- I will not access other people's files on the school system.
- I will not intentionally damage any ICT equipment, and will report any damage I find to a member of staff.
- I will not use inappropriate language in any of my documents.
- I will only use my school email address in school and at times that are directed by my teacher.
- I will only email people I know, or people that my teacher has approved.
- I will only send email in my name, and will not send any anonymous email.
- The email messages I send will be appropriate in content and not likely to cause offence to anyone.
- I will report to a member of staff any messages that are unpleasant, offensive or cause discomfort to me.
- I will not provide personal or contact details, or those of my friends to anyone outside of the school.
- I will not arrange to meet someone through a contact made over the Internet/Intranet.
- I will only access appropriate Internet sites.
- If I find inappropriate material on a website I will immediately inform a member of staff.
- Users must not use the school ICT systems / network for the access of, creation of, or transmission of content that promotes extremist activity, including terrorism, radicalization and weapons.
- I understand that the school has the ability and may use it regularly to monitor my activities on-line and check my computer files, any emails I may send or receive, and any Internet sites I visit.
- I understand that the improper use of the school computers and network will be considered a serious breach of school discipline and trust, which may result in me, in the first instance, being refused permission to use the system. Additional sanctions will be applied as appropriate, including exclusion from school. Parents will be informed as a matter of routine and the police will be asked to take appropriate action where it is believed that an offence may have been committed.

Ask your ICT teacher to explain anything that you do not fully understand.

Signed: ……TG: ……House:…….

Print Name: ……**Date:** …….

Appendix 2 - Login script

This statement appears on the pre-login screen and OK has to be clicked before students or staff can Login:

'Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied and disclosed to senior members of staff and if deemed law enforcement personnel. By using this system, the user consents to such interception, monitoring, recording, copying and disclosure at the discretion of The Warriner School. Unauthorized or improper use of this system may result in disciplinary action and criminal penalties. By continuing to log on you are accepting this agreement.'

Appendix 3 - Responsible Internet Use at The Warriner School

All students use computer facilities at The Warriner School including Internet access as an essential part of learning, as required by the National Curriculum. Both students and their parents/carers are asked to sign the Rules for Responsible use of Computers in School to show that e-Safety Rules have been understood and agreed.

Although there are concerns about students having access to undesirable materials, we have taken positive steps to reduce this risk in school. We operate a filtering system that restricts access to inappropriate materials. This may not be the case at home and we can provide references to information on safe Internet access if you wish.

We also operate a hardware screening system that scans files, folders and emails for inappropriate language based on Key Words.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Appendix 4 - Staff Information Systems Code of Conduct

Staff should consult the school's E-Safety, Internet and Acceptable Use Protocol for further information and clarification.

The information systems are school property and staff should understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- Staff will ensure that the use of information systems will always be compatible with their professional role.
- Staff should understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- Staff should understand that the school may monitor use of information systems and the Internet to ensure policy compliance.
- Staff must respect system security and will not disclose any password or security information to anyone.
- Staff should not install any software or hardware without permission.
- Staff will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- Staff will respect copyright and intellectual property rights.
- Staff will report any incidents of concern regarding children's safety to the school e-Safety Coordinator (relevant Senior Leadership Team member) or the Designated Child Protection Coordinator.
- Staff will ensure that any electronic communications with students are compatible with their professional role.
- Staff will promote e-safety with students in their care and will help them to develop a responsible attitude to system use and to the content they access or create.
- Users must not use the school ICT systems / network for the access of, creation of, or transmission of content that promotes extremist activity, including terrorism, radicalization and weapons.
- The school will exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- Inappropriate use of the ICT facilities including accessing inappropriate content on the Internet may result in disciplinary action.