Uffington Church of England Primary School

'Optimum Solum Satis Est' – 'Only the best is good enough'

ACCEPTABLE USE OF ICT / E-SAFETY POLICY

Acceptable Use Statement

The computer system is owned by the school. "The computer system" means all computers and associated equipment belonging to the school.

Professional use of the computer system is characterised by activities that provide children with appropriate learning experiences; or allow adults to enhance their own professional development. The school recognises that technologies such as the internet and e-mail have a significant effect on children's education and staff professional development and the school's e-Safety Policy has been drawn up accordingly.

The installation of software or hardware unauthorised by the school, whether legitimately licensed or not, is expressly forbidden.

The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited.

All children must be made aware through class discussion of all the important issues relating to acceptable use, especially the monitoring of Internet use.

All staff should sign an information systems code of conduct on appointment. Staff thereby accept that the school can monitor network and Internet use to help ensure staff and pupil safety. All staff have a responsibility to report inappropriate or illegal ICT use to senior management.

A member of staff who flouts security advice, or uses email or the internet for inappropriate reasons risks dismissal.

E-Safety Policy

What is e-Safety?

The School's e-Safety policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole. e-Safety encompasses not only internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and

responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.
The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.
Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others.
Schools need to protect themselves from legal challenge although the law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to 'groom' children.

Although the school will endeavour to protect itself by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised", it is aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

What does electronic communication include?

- **Internet collaboration tools:** social networking sites and web-logs (blogs)
- **Internet research:** websites, search engines and web browsers
- **Mobile phones and personal digital assistants** (PDAs)
- **Internet communications:** e-mail and IM
- **Webcams and videoconferencing**
- **Wireless games consoles**

What are the risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Hacking and security breaches
- Corruption or misuse of data

Responsibilities of school staff

The e-Safety Co-ordinator will:

- maintain the e-Safety Policy, manage e-Safety training and keep abreast of local and national e-safety awareness campaigns;
- review policy regularly to ensure that it is current and considers any emerging technologies;
- ensure that pupils and staff are adhering to the policy, investigating any incidents of possible misuse;
- discuss opportunities for teaching e-Safety in the curriculum with staff and ensure that every pupil has been educated about safe and responsible use;
- ensure that all staff read and sign the Information Systems Code of Practice;
- ensure that the e-Safety Policy is made available to all staff, governors, parents and visitors.

The Headteacher takes the role of e-Safety Co-ordinator at Uffington School.

Teaching and Learning

Why is Internet use important?

- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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.
- Pupils use the internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the local authority and the Department for Education;
- access to learning wherever and whenever convenient.

How can internet use 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.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate Internet content?

It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

Respect for copyright and intellectual property rights, and the correct use of published material should be taught. The schools will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Managing Information Systems

How will information systems security be maintained?

- Workstations should be secured against user mistakes and deliberate actions.
- The server is located in the administrator's office to ensure security and restrict physical access;
- The server operating system is secured and kept up to date by Mouchel Business Services;
- Virus protection for the whole network is installed centrally and kept up to date by Mouchel Business Services;

Wide Area Network (WAN) security

- The school's internet connection is arranged via the local authority to ensure compliance with the security policy.
- The security of the school information systems will be reviewed regularly and strategies discussed with the local authority.
- Personal data sent over the internet will be encrypted or otherwise secured.

- Portable media may not be used without specific permission; the preferred method of data transfer is via e-mail although USB sticks and DVDs may be used where there is an issue regarding file size.
- Files held on the school's network will be regularly checked.
- The ICT co-ordinator / network manager will review system capacity regularly.

How will e-mail be managed?

- Pupils may only use their approved e-mail account through the Assimilate Learning Platform.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

How will published content be managed?

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

- Images 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 images of pupils are electronically published *(see Photographic Consent Policy)*
- Work can only be published with the permission of the pupil and parents.

How will social networking and personal publishing be managed?

- The school will block access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space.

How will filtering be managed?

- The school will work with their IT provider to ensure that systems to protect pupils are reviewed and improved to ensure that filtering methods are appropriate, effective and reasonable.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e-safety Coordinator.
- Any material that the school believes is illegal will be reported the local authority.

How can emerging technologies be managed?

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

How should personal data be protected?

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

Policy Decisions

How will internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.
- At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised internet access.

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Lincolnshire County Council can accept liability for the material accessed, or any consequences resulting from Internet use.

- The school will audit ICT use to establish if the e-Safety Policy is adequate and that the implementation of the policy is appropriate.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

- Methods to identify, assess and minimise risks will be reviewed regularly.

How will e-safety complaints be handled?

- Complaints of internet misuse will be dealt with by the Headteacher.

- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the general complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy include:
  – informing parents or carers;
  – removal of internet or computer access for a period.

How is the internet used across the community?

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

How will the policy be introduced to pupils?

- Pupils will be informed that network and internet use will be monitored.
- Instruction in responsible and safe use should precede internet access.
- An e-safety module will be included in the PSHE and Citizenship curriculum covering both school and home use.

How will the policy be discussed with staff?

- All staff will have access to the School e-Safety Policy and its application and importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible internet use and on the school e-Safety Policy will be provided as required.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.

……..

This policy has been agreed by the staff and Governing Body and is reviewed biennially.

Policy created and adopted by the Governing Body	November 2014
Policy revised and agreed by the Curriculum and Standards Committee	October 2015
Policy revised and agreed by the	December 2016

Curriculum and Standards Committee	
Next Review	November 2018