



St. Mary's Catholic High School

An 11 to 18 Specialist Mathematics and Computing College

E-Safety Policy

Approved by Full Governing Body: February 2011

Signature:

Next Review Date: June 2012

Staff Responsible: Mr Tony Jones

Manchester Road Astley Tyldesley Manchester
Tel: 01942 884144
Fax: 01942 884357
Email: enquiries@admin.st-maryshigh.wigan.sch.uk

E-Safety Policy

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 information and business administration systems.

Internet access is an entitlement for students who show a responsible and mature approach to its use.

The Internet provides:

- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between students world-wide
- Cultural, vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for students and staff
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues; improved access to technical support including remote management of networks.
- Exchange of curriculum and administration data with the LA and the DfES.
- Access to the school virtual learning network, allowing collaboration with colleagues within the LA and nationally.

How will Internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of students.
- Students 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 students.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
- Students at Key Stage Three, Four and Five will be educated in the effective use of the Internet for research, including the skills of knowledge location, retrieval and evaluation.

How will students learn to evaluate Internet content?

- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Network Manager/Deputy Network Manager in the first instance. The URL will be evaluated to determine if it is indeed unsuitable, and will be filtered accordingly.
- Schools should ensure that the use of Internet derived materials by staff and by students complies with copyright law.

- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will e-mail be managed?

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive an offensive e-mail.
- Students must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and will be restricted.
- The forwarding of chain letters is not permitted.

How should Web site content be managed?

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or students' home information will not be published.
- Web site photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- The headteacher or nominee will take overall editorial responsibility and ensure that the content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Can Chat/Message boards be made safe?

- Students will not be allowed access to public or unregulated chat rooms.
- Students should use only regulated educational chat environments/message boards. This use will be supervised and the importance of chat room safety emphasised.

How can emerging Internet applications be managed?

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

How will Internet access be authorised?

- The school will keep a record of any students whose parents have specifically denied internet or e-mail access.

- Students at Key Stage Three, Key Stage Four and Key Stage Five will be provided with supervised Internet access.
- Parents will be asked to sign and return a form stating that they have read and understood the acceptable use policy.

How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet 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 LA 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.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will filtering be managed?

- The school will work in partnership with parents, the LA and the DfES to ensure systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported the Network Manager/Deputy Network Manager.
- Filtering strategies will be selected by the school, in discussion with Wigan LA. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

How will the policy be introduced to students?

- Students will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Students will be reminded of the rules and risks at the beginning of any lesson using the Internet.

How will staff be consulted?

- All staff are governed by the terms of the 'Responsible Internet Use' in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the school Internet policy, and its 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 development in safe and responsible Internet use and on the school Internet policy will be provided as required.

How will ICT system security be maintained?

- The school ICT systems are reviewed regularly with regard to security.
- Virus protection is installed and updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.

- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
- Files held on the school's network will be checked regularly.

How will issues regarding E-Safety be handled?

In the event of an E-safety issue, the procedure outlined on the flowchart on page 6 of this document should be consulted.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school Internet policy in newsletters, the school prospectus and on the school Web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

How is Internet used across the community?

- Adult users will need to sign the acceptable use policy, and agree to this each time they log on to the school system.
- Parents/carers of children under 16 years of age will be required to sign an acceptable use policy on behalf of the child.

How will forensic monitoring software help to make computer systems safer?

- Forensic monitoring software (Securus) is in place on every computer and laptop in school and provides dynamic monitoring for several "bad word libraries" which once triggered, takes a screenshot of the material being accessed and records the user who accessed the information, the time, date and also computer used. This allows e-safety issues such as bullying, access of inappropriate materials via the Internet or locally to be monitored effectively.
- Securus provides users with a copy of the school's acceptable use policy on logon and should the user disagree, they are logged out of the system immediately. If they agree, they are allowed access to the school systems as normal.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If Illegal activity is suspected, evidence gathering and preservation must be carried out by the nominated person in charge of e-safety (Deputy Network Manager) along with the network manager Evidence should only be printed out in hard copy if printing out does not in itself be construed as an illegal act

Once evidence gathering has been performed, it should be kept in a secure location for the authorities to examine, and the user in question should have their access rights to the school systems revoked immediately to prevent any further misuse.

If a student or a member of staff has been found to have no illegal material or activity attributed to them, then internal disciplinary procedures should be followed if the material is unsuitable for the school network.

Key staff members:
 Child protection officer: D. Brahms
 School based police officer

E-Safety Issue



