The Island Learning Centre
Online Safety Policy

Published February 2020
To Be Reviewed by February 2021

Grainne Andrews
Chair of the Management Committee

One of three documents:
1. ICT Policy
2. Online Safety Policy
3. Staff Acceptable Use of ICT

Who will write and review the policy?

The Designated Safeguarding Lead will be responsible for all issues regarding Online Safety:

- The Online Safety Policy and its implementation will be reviewed annually.
- The School is committed to ensuring the safety of pupils when they are using ICT in the wider world.

Teaching and Learning

Why is Internet use important?

Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is a part of everyday 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 need to learn how to evaluate Internet information and to take care of their own safety and security.

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

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

The school's Internet access will be designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to online 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.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The evaluation of online materials is a part of teaching/learning in every subject.

Managing Information Systems

How will information systems security be maintained?

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed.

The security of the school information systems and users will be reviewed regularly.

Virus protection will be updated regularly.

- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- IOW IT (Data Swift) will review system capacity regularly.

How will email be managed?

- Pupils may only use approved email accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

Access in school to external personal email accounts may be blocked.

- Excessive social email use can interfere with learning and will be restricted.
- Email 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 messages is not permitted.
- Schools may have a dedicated email for reporting wellbeing and pastoral issues and this inbox must be approved and monitored by members of Senior Leadership Team.
- Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team.
- Staff should not use personal email accounts during school hours or for professional purposes.

How will published content be managed?

The contact details on the website should be the school address, email 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 provide material that could be used.
- 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.

How will social networking, social media and personal publishing be managed?

The school will control access to social media and social networking sites. Pupils will be 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 email addresses, full names of friends/family, specific interests and clubs etc.

- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- If personal publishing is to be used with pupils then it must use age appropriate site suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others by making profiles private.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

How will filtering be managed?

If staff or pupils discover unsuitable sites, the URL must be reported to the Designated Safeguard Lead. The school's broadband access will include filtering appropriate to the age and maturity of pupils.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils.

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.

- Mobile phones will not be used during lessons or formal school time without the permission of a member of staff. The sending of abusive or inappropriate text, picture or video messages is forbidden.

How should personal data be protected?

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Held no longer than is necessary
6. Processed in line with individual's rights
7. Kept secure
8. Transferred only to other countries with suitable security measures.

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

<u>Policy Decisions</u>

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. For some pupils access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online

materials. Other pupils must apply for Internet access individually by agreeing to comply with the Online Safety Rules. Parents will be asked to sign a consent form for pupil access during induction.

- 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 IOW Council can accept liability for the material accessed, or any consequences resulting from Internet use.

- 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 Online Safety complaints be handled?

Any complaint about staff misuse must be referred to the headteacher. All Online Safety complaints and incidents will be recorded by the school — including any actions taken.

- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.
- Parents and pupils will work in partnership with staff to resolve issues.

How is the Internet used across the community?

- 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 Cyberbullying be managed?

Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying. There will be clear procedures in place to support anyone affected by Cyberbullying.

- All incidents of cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include:
  - The bully will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content.
  - Internet access may be suspended at school for the user for a period of time.
  - Parent/carers may be informed.

- The Police will be contacted if a criminal offence is suspected.

Communication Policy

How will the policy be introduced to pupils?

All users will be informed that network and Internet use will be monitored.

- Pupil instruction in responsible and safe use should precede Internet access.
- An Online Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- Online Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

The Online Safety Policy will be formally provided to and discussed with all members of staff. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- All staff will receive a copy of Staff Acceptable Use of ICT.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

How will parents' support be enlisted?

Parents' attention will be drawn to the School Online Policy in newsletters and on the school website.

- Parents will be requested to sign an Acceptable Use of ICT Agreement upon induction.
- Information and guidance for parents on Online Safety will be made available to parents in a variety of formats.