E-Safety Policy

Author: Catherine Beard, Senior QA Lead

Policy Responsibility: James Brown, Head Teacher

Date approved: 1st August 2023

Review Date: Annual, by 1st August 2025

Version: 1

Location: Policy Folder (Digital & Hardcopy), Staffroom, Website

Introduction

The e- Safety Policy is part of the ICT Policy and the School Development Plan, it relates to other policies including those for Computer Science, Positive behaviour, RSE, social and health education (PSHE) and citizenship.

The school has appointed an e-safety Co-ordinator- James Brown who is also Designated Senior Lead for Safeguarding as well as being the SENDCo.

Why does Ormston School need an e-Safety Policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

E-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Schools and other settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. Schools must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an e-Safety policy can and have led to civil, disciplinary, and criminal action being taken against staff, pupils, and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have.

Schools must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and the Governing body.

The e-Safety policy is essential in setting out how the school plans to develop and establish its e-Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

Internet Use

The rapid development in electronic communications is having many effects on society. The internet is an essential element in 21st century life for education, business, and social interaction. At this present time, every child in school has access to the internet at school and the majority go on-line at home. Many use it more often and with more expertise than adults.

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

Internet use is a part of the statutory curriculum and is a necessary tool for staff and pupils. The school has a duty to provide students with quality internet access as part of their learning experience.

How the Internet benefits learning

Benefits of using the internet in learning include:

- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between pupils world-wide
- Cultural, vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for pupils 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 LEA.
- The use of virtual learning environments (VLEs) for children to communicate and collaborate with other children across the world e.g. think.com
- The use of video conferencing to access resources and cultural exchanges around the world
- Exam access and revision access

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 the pupils.

Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for internet use. They will be educated in the effective use of the internet in research, including the skills of knowledge location and retrieval.

How will the pupils learn to evaluate Internet content?

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the James Brown via email, and he will contact the school's ICT support team.

We will ensure that the use of the internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to acknowledge the source of information and to respect copyright when using internet material in their own work.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will need to learn how to evaluate internet information and to take care of their own safety and security.

Training should be available to staff in the evaluation of web materials and methods of developing student's critical attitudes.

Email

Pupils may only use approved email accounts on the school system. Pupils can email within the school's email addresses but only when an adult opens the system can they email outside of those email addresses.

Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in any online activity. All pupils have email safety lessons throughout the year. There are also age-appropriate sessions on other aspects of online safety such as cyber bullying, grooming and CSE.

Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed notepaper.

Pupils must immediately tell a teacher if they receive offensive email.

Excessive social email use can interfere with learning and may be restricted. The forwarding of chain letters is banned.

Social Networking

Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.

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

Pupils should be advised not to place personal photos on any social network space.

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.

Website content

The point of contact on the Web site should be the school address, school email and telephone number. Staff or pupils' personal information will not be published.

Web site photographs will be selected carefully, and any photos of pupils will not identify them

Pupils' full names will not be used anywhere on the Web site.

Written consent from parents or carers is obtained before photographs of pupils are published on any media from the school e.g. the newsletter.

The Polaris IT lead will take overall editorial responsibility and ensure content is accurate and appropriate in collaboration with the Head teacher.

The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Publishing Pupils' Images and Work

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 Web site or Blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site

Work can only be published with the permission of the pupil and parents.

Chat rooms

Pupils will not be allowed access to public or unregulated chat rooms. Children should only use regulated educational chat room environments. This will always be supervised and the importance of chat room safety emphasised.

Emerging Internet uses

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 not be used at school. Children who do bring mobile phones to school are asked to leave them in the office until home time.

Internet access

Parents will be informed that pupils will be provided with supervised internet access. Pupils and staff will be asked to agree and to abide by the Responsible Internet Use statement.

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 pupils. 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 the internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SI Solutions 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, access and minimise risks will be reviewed regularly.

The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

How will filtering be managed?

The school will work in partnership with the parents to ensure systems to protect pupils are reviewed and improved.

Filtering and Firewall is managed by Sensible It Solutions

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported immediately. Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The Prevent Duty and Online safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well being of any pupil is being compromised.

All staff are trained to look for signs of extreme views and possible online activity which may lead to concern. School have robust systems in place to report the concern and support the individual pupil.

How will the policy be introduced to pupils?

Rules for Internet access will be posted near all computer systems.

Pupils will be informed that Internet use will be monitored.

Instruction in responsible and safe use should precede Internet access.

Pupils have e safety sessions in school

Staff

All staff must accept the terms of the Responsible Internet Use statement before using any resource 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 could be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff development in safe and responsible internet use, and on school Internet policy will be provided as required.

All staff will be trained in Safeguarding procedures, including elements of Online safety and The Prevent Duty.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

ICT system security

The school ICT system will be reviewed regularly with regard to security.

Virus protection will be installed and updated regularly Security strategies will be discussed with the LA.

The coordinator will ensure that the system has the capacity to take increased traffic caused by internet use.

Complaints regarding Internet use

Responsibility for handling incidents will be delegated initially to the co-ordinator. All concerns should be logged using the schools information sheet procedures.

Any complaint about staff misuse must be referred to the head teacher.

As with drug issues, there may be occasions when police may be contacted. Early contact could be made to establish the legal position and discuss strategies.

Parents support

Parents' attention will be drawn to the School Internet policy in newsletters, the school brochure and on the school website.

Internet issues will be handled sensitively to inform parents without undue alarm.

Useful e–Safety programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Orange Education: www.orange.co.uk/education
- Safe: www.safesocialnetworking.org