Oriel High School : ICT & E-Safety Policy

Date Amended: September 2024 **Date of Ratification: 25.09.24**

Next Review Date: September 2025

Aim

ICT plays a critical role in the day-to-day experience of all staff and students at Oriel High School, from specific Teaching and Learning applications through to internet use, data systems and communications. As such, it is important that this document clearly highlights where policy and procedures are required to maximise the efficiency of these applications and yet also ensure that risks, both technical and personal, are managed effectively

The school has appointed an E-Safety co-ordinator who is responsible for ensuring the implementation of this policy and for leading the review of this policy on an annual basis in collaboration with key personnel including the Child Protection Officer, Business Manager, Director of E-Learning, Network Manager, the Subject Leader for ICT and the designated governor responsible for E-Safety.

Rationale

The use of the ICT and use of the internet is not only a statutory requirement of the curriculum, but it is a necessary tool for learning. It is also a part of everyday life for education, business and social interaction. As such the school has a duty to provide students with quality internet access as part of their learning experience. With the proliferation of internet access on mobile devices such as phones and tablets, as well as through PCs and laptops, it is of critical importance that students learn how to evaluate internet information and how to take care of their own safety and security.

Key Staff

Helen Everitt : Deputy Headteacher (E-Safety Co-ordinator)
Ben Cleaveley : ICT Subject Leader
Steve Harris : IT Network Manager
Ryan Sallows : Business Manager

The Internet

All school PCs have networked internet access provided by the school. This provides a filtered service with all students having a school login and email account.

The school's internet access is designed to enhance and extend the educational experience of students and enable quality teaching resources, data management and staff training.

Students will be taught:

- what internet use is acceptable and what is not, and they are given clear learning objectives and outcomes for all internet use in lessons
- to acknowledge the sources of information used and to respect copyright when using internet material in their own work
- to be critically aware of the materials that they read and will be shown how to validate information before accepting its accuracy

This final aspect is the joint responsibility of all subjects asking students to use the internet and will therefore be viewed as a whole-school requirement across the curriculum.

Filtering

The school's broadband access will include filtering appropriate to the age and maturity of the students, and this includes blocking all sites on the Internet Watch Foundation (IWF) list. The school has a clear procedure for reporting breaches of filtering and this is laid out in the Acceptable Use Policies for both staff and students. The E-Safety Co-ordinator and the Network Manager will record and act upon all reports of breaches of filtering.

There may be occasions when individual staff may require certain sites or resources to be available to students for a specific educational purpose. In cases such as this, the staff concerned should discuss the rationale with the E-Safety Co-ordinator before any decision is made to unblock sites.

It is important that all staff in the school recognise that filtering is not 100% effective and all use of the internet in school should be closely supervised, remembering that a site which is considered safe one day may be changed when next accessed. Particular attention should be paid to advertisements as these can change each time a page is accessed.

Managing Systems

The security of the school network and systems will be regularly reviewed with corresponding virus protection updates. Personal data sent over the internet or taken off-site will be encrypted. Software is installed by the IT Network Manager that enables portable media devices to be scanned before being accepted onto any networked machine.

Software is not to be individually downloaded onto any networked machine; all software installation must be completed by the IT Network Manager following a full evaluation.

Files held on the school system will be regularly checked and the system capacity will be reviewed accordingly with clear limits on the amounts of data storage available.

The use of user logins and passwords to access the school network will be enforced with passwords changed at regular intervals.

All personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. A careful approach to parental access to Go 4Schools will be required to ensure the data Act conformity.

Email Communication

Email is an essential means of communication for both staff and students and yet it is important that appropriate safety systems are in place. All staff and students are given an official email account that will restrict incoming mail and filter unsuitable content. In the school context, email should not be considered private and the school reserves the right to monitor email, balancing the necessary monitoring to ensure the safety of students and staff and the preservation of human rights.

Student email accounts will not identify their full name and school. In ICT lessons, students will be taught that they:

- must immediately inform a member of staff if they receive an offensive email in their school account
- must not reveal personal details of themselves or others in email communication
- must not arrange to meet anyone they do not personally know

Staff will:

- use only the official school-provided email accounts to communicate with students and parents/carers
- not be able to access external personal email accounts
- avoid excessive social email on the school system

- ensure that emails sent to external organisations will be written carefully and, in some situations, authorised before being sent in the same way as a letter written on school headed paper would be
- not forward chain messages
- not use personal email accounts from home or mobile devices for school purposes

Published Content

The school has invested in the development of its website and online presence. As such, it will be seeking to inspire students by displaying work of a high standard in order to celebrate their achievement and promote the school. Also its intention is to provide high quality communication with parents.

The Headteacher will take overall editorial responsibility for all online content published.

Any newsletters or information sent via Parentmail or posted on the school website will always be considered from a personal and school security viewpoint.

The contact details on the main website will only be the school address, email and telephone numbers. Staff and students' personal contact details will never be published.

Images or videos that include pupils will be selected carefully and will be re-sized wherever possible to minimise the risk of external downloading and re-use of images and videos.

Students' full names will not be used anywhere on the website, in association with photographs. Parents will have the right to deny permission for images of their son/daughter to be published and the school will keep records of where this consent is denied.

Related document: "Photographs/Images of Students Statement"

Social Media

Parents and teachers need to be aware that social networks allow individuals to publish unmediated content which other users can view and leave comments upon, over which there is limited control. However, there are occasions when blogs and discussion forums are valuable educational tools, but these need to be carefully assessed by staff before being used. Various features are available in Moodle and these should be investigated first.

In addition to this, there are websites which offer shared blogging facilities with supervisor control. Official blogs or WIKIs should be risk assessed, password protected and run from the school with approval from the SLT. Staff should never run social network spaces for students' use on a personal basis.

The school will provide guidance to students, parents and staff in the safe use of social media and social networking while still controlling access to social media and social networking sites. Guidance will include the fact that no-one should give out personal details of any kind which may identify them and/or their location (e.g. full names, address, mobile or home phone numbers, school attended, IM and email addresses, full names of family and friends etc.), that users are to approve and invite known friends only, are to deny access to others by making their profiles private, and also how to manage specific functions of new technologies (e.g. Facebook places) and personal publishing sites (such as flickr).

Concerns regarding an individual student's use of social networking, social media and personal publishing sites will be raised with their parents/carers.

Staff guidance will include advice on social media and social networking as well as the Acceptable Use Agreement, and this will form a part of staff induction.

Emerging and New Technologies

New applications, communication technologies and software are constantly being developed and opened up to schools for use as potential teaching and learning tools. This includes mobile communication, collaboration and multimedia tools. It is important that a new application is effectively appraised for potential risks before being introduced into the classroom. This should be done in collaboration with the Assistant Headteacher (E-Learning) who will then evaluate with the IT Network Manager if appropriate

Approaches such as mentoring, online learning and parental access are becoming more and more a feature for schools and they all can have a powerful impact upon students and the progress they can make. However, the safety and effectiveness of these applications depends upon users being trusted and also identifiable. This is not easy as authentication beyond the school may be very difficult. It is important to ensure that any application that the school employs does not blur these lines; any application used or sanctioned by the school should only be used when authentication of user identity is secure.

As a school, we will endeavour to keep up to date with new and emerging technologies, including those relating to mobile devices, and be ready to develop strategies when and if a need arises.

Anti-Bullying Policy

All forms of bullying in the school, including "the use of ICT, particularly mobile phones and the internet, to deliberately hurt or upset someone" will not be tolerated and full details of the school's approach are set out in the policy on anti-bullying and behaviour. The school does not make a distinction between this and any other forms of bullying.

As a school we have specific resources within the PDC Curriculum that educates students on this issue and this will be expanded to incorporate new technologies as and when they become necessary. This is delivered alongside E-Safety elements of the PDC and ICT Curriculum. The school's expectations towards this are also clearly stated in the behaviour policy.

All bullying of this form that is reported to the school will be investigated using the normal procedures and recorded in the same way as any other incident of bullying, and normal sanctions will always apply.

PREVENT: The Issue of Radicalisation

The Counter-Terrorism and Security Act 2015, places a legal responsibility on schools to take every effort to protect members of their community from the threat of political radicalisation. We approach this issue in four ways:-

Providing a Safe Online Environment: The school has strong filters in place to block student access to violent or otherwise inappropriate materials. Students are required to sign an Acceptable Use of ICT policy that specifically prohibits them from seeking to access such sites. Internet usage is monitored and pastoral and/or disciplinary responses may follow if a student's usage breaches our rules or raises concerns.

The school will also seek to block specific sites and search terms too if they appear to pose a risk to our students. Furthermore, students will receive advice and instruction from teaching and pastoral staff on safe internet usage.

Assessment of Student Behaviours: The pastoral monitoring systems of the school have a vital role to play in preventing radicalisation of students. At Oriel High School students are monitored closely by Mentors and Heads/Deputy Heads of Learning Communities and issues of concern are discussed at the weekly pastoral meeting. Where necessary pastoral intervention or even counselling may be provided. The school will also seek advice and support from the local authority when concerns regarding pupil radicalisation arise.

Staff Training and Information: The school recognises that it has a responsibility to provide INSET to staff on the issue of radicalisation to ensure that they remain vigilant and informed on the issue. It will also ensure staff are aware of how to respond appropriately if concerned about the possible radicalisation of a student.

Promoting Fundamental Values: The school will vigorously promote fundamental values such as fairness, democracy, tolerance and the rule of law through its PSHE Programme, its tutorial programme and assemblies, the curriculum and all other daily interactions between students and staff.

Contacts and Resources: Government advice to schools on this issue can be accessed here: https://www.gov.uk/government/publications/preventing-extremism-in-schools-andchildrens-services

The Government also provides contact details for alerting authorities to suspected terrorist activity. These include the DfE dedicated telephone helpline and mailbox for non-emergency advice for staff and governors: 020 7340 7264 and counter-extremism@education.gsi.gov.uk in addition to the local police and 101.

Mobile Phones and Personal Devices

Mobile phones and other devices (such as tablets, MP3 players etc.) are an everyday item now in society and students will own and use these devices. The development of this technology means that students will be able to access the internet, record images and communicate with others outside of the school network. This presents a number of risks:

- These items are generally quite expensive and so issues of theft or damage may arise
- Internet access will bypass the school's filtering procedures
- They can potentially undermine classroom discipline
- Capture of inappropriate images may lead to bullying, data protection or even child protection issues.

Within this policy it is important to recognise that issues relating to mobile phone safety are part of a co-ordinated approach to E-Safety and bullying. The PDC programme will incorporate elements of mobile phone safety, and information will be made available to parents through the school website and additional contact indicating the E-Safety issues surrounding mobile phone use.

Policy Implementation

Any additions or changes to this E-Safety policy will be raised with staff following ratification by the full governing body at which point they will be asked to sign the Acceptable Use Agreement. Staff will be expected to sign this agreement every time the policy is altered.

Students will be introduced to this policy through the requirement to sign an Acceptable Use Agreement at the beginning of each academic year, or upon admission if they are an in-year admission.

Copies of the Students' Acceptable Use Agreement (AUA) will be prominently displayed in all ICT Rooms and will be posted on the school website.

Resources and Facilities

Key personnel will regularly review and update the strategic plan for upgrading the provision of ICT equipment, software and facilities across the school for both staff and students. Priorities will be included and identified in school budgetary planning.

Related School Policies:

Anti-Bullying	Health & Safety
Attendance	Safer Recruiting
Behaviour	SEND
Confidential Reporting	Sex Education
Child Protection & Safeguarding	Substance Use and Abuse
Equalities	Use of Photography and Recording