OAKWOOD PARK GRAMMAR SCHOOL

E-Safety Policy

Approval status	Approved
Last reviewed on:	September 2023
Next review due on:	September 2026

Introduction

The curriculum requires students to learn how to locate, retrieve and exchange information using IT. Teachers need to plan to integrate the use of technology such as web-based resources and email. IT skills are vital to access life-long learning and employment.

Technologies present risks as well as benefits. Internet/social networking use for work, home, social and leisure activities is expanding in all sectors of society. This brings students into contact with a wide variety of influences, some of which may be unsuitable. Unmediated Internet access through computers, telephones and iPads etc. brings with it the possibility of placing students in embarrassing, inappropriate and even dangerous situations.

Refer to OPGS Safeguarding Policy, including sections on Preventing Radicalisation/Extremism & Filtering and Monitoring.

Core Principals

- Guided Educational Use – Curriculum internet use should be planned, task-orientated and educational within a regulated and managed environment.
- Risk Assessment – Students must be protected from danger (violence, racism, exploitation) and learn how to recognise it.
- Responsibility – All staff, governors, external providers, parents and students must take responsibility for the use of the Internet.
- Regulation – In some cases eg. Unmoderated chat rooms, immediate dangers are presented, and their use is banned. In most cases strategies on access must be selected and developed to suit the educational activities and their effectiveness monitored. The Senior Team will determine which websites are blocked.
- This policy is closely related to the guidance contain in; Keeping Children Safe in Education – statutory guidance to schools and colleges. Keeping children safe in education 2023 (publishing.service.gov.uk)
- With regards to Radicalisation via the internet and social media the school fully adopts The Prevent Duty – departmental advice for schools and childcare providers.

Importance/Benefits of Internet Use

- Raise educational standards, promote pupil achievement.
- Support work of staff and enhance management systems.
- Part of the curriculum and a necessary tool in teaching and learning.
- Students are entitled to quality Internet access as port of their 21st century learning experience.
- Access to worldwide resources and experts.
- Educational and cultural exchanges between students worldwide.
- Facilitate staff professional development.
- Communication with external services.
- Exchange of curriculum and administrative data/sharing of good practice.

Ensuring Internet Use Enhances Learning

- Internet access with be designed expressly for student use and will include filtering appropriate to students' ages.
- Students will be taught what is acceptable and what is not acceptable and given clear learning objectives when using the Internet.
- Internet use will be planned to enhance and enrich learning. Access levels and online activities will be provided and reviewed to ensure they reflect curriculum requirements and student age.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Student Evaluation of Internet Content

- Any user discovering unsuitable sites must report the address and content to; the Internet Service Provider, the IT Support Staff, a teacher or the Designated Child Protection Co-ordinator as appropriate.
- The use of the Internet derived materials must comply with copyright law.
- Students will 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 and to respect copyright when using Internet material in their own work.

Management of Email

- Pupils may only use approved email accounts on the school system.
- Access in school to external personal email accounts will be blocked for all students.
- Pupils must immediately tell a teacher if they receive offensive emails.
- Pupils must not reveal details such as address/telephone number of themselves or others or arrange to meet anyone in email communication.
- Social email can interfere with learning and will be restricted.
- Email sent to an external organisation should be carefully written and authorised by a teacher before sending.

Management of the School Website Content

- The point of contact on the website is the school address, email and telephone number. Staff and students' home information will not be published.
- Use of photographs showing students and students' names will not be used on the website without parental consent.
- The Deputy Headteacher responsible for IT systems, acting as the Headteacher's nominee, will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Social Networking/Media

- Only employees who have been authorised to use social media accounts by the Head Teacher may access social media on the School's network or create, maintain, or post on behalf of school accounts.
- The use of social media will only be approved where it is deemed to benefit learners and learning, is in the business interests of the school, and meets safeguarding and PREVENT duties.
- Only employees who have been authorised by the Head Teacher may encourage students to access social media accounts which are relevant to their learning.

Managing Emerging Technologies

- 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 the rest of the school day) unless they provide a benefit to students' education.
- The school's Video Conference facility and video cameras may only be used by the students for educational use under staff supervision.
- The school has acceptable use guidance for the use of Microsoft Teams. All such material and guidance will be reissued in the event of a switch to remote learning.

Authorisation of Internet Access

- The school will maintain an up-to-date record of all staff and students who are granted internet access.
- All internet access is monitored and recorded using electronic means.
- All staff and students (and students' parents) must read the Acceptable Use Policy. AcceptableUse.pdf (opgs.org)
- Inappropriate use of the internet will be dealt with in accordance with the school's Behaviour Policy.

Risk Assessment

- Some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure such material is not accessed by students. However, it is not possible to guarantee that such material will never appear on a school computer – Oakwood Park Grammar School cannot accept liability for material accessed or any consequences of Internet access.
- The use of computer systems without permission or for the inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risk will be reviewed regularly.

Management of Filtering & Monitoring

- The school will work in partnership with parents, the DfE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- Any Internet user must report unsuitable/illegal sites to the Deputy Head responsible for IT (and the Designated Teacher i/c Child Protection if necessary) immediately.
- The Deputy Headteacher with the IT Support Staff will oversee regular checks to ensure that the filtering methods used are appropriate, effective and reasonable. Content is filtered using 'Sophos' and communications are monitored through 'Sophos' and 'senso.cloud'.

- If filtered websites need to be used by staff, they must inform IT Support to have them unblocked for a set period of time.
- IT Support Staff will ensure flags on inappropriate searches are sent to the relevant Deputy Headteachers.

IT System Security

- The school's IT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Files held on the school's network will be regularly checked.
- Use of portable media such as memory sticks and CD's will be reviewed regularly.
- Downloading of unauthorised files will be prohibited, and where possible blocked.
- Use of the school's IT systems will be subject to the Data Protection Act, the Computer Misuse Act and General Data Protection Regulation.

Student, Staff and Parental Awareness

- All stakeholders will be made aware of this policy and how it relates to them.
- All staff will read the Acceptable Use Policy
- All students will read the Acceptable Use Policy – it will also be issued to parents.
- Rules for Responsible Computer and Internet Use will be posted near all computer workstations.
- Students will be instructed in responsible and safe internet use before being granted access.
- Responsible use of the internet, including social networking will be discussed through the PSHE and Digital Literacy programmes, covering use in school and outside of school.
- The monitoring of internet use is a sensitive matter – staff who operate monitoring procedures will be supported by IT Support Staff and responsible Deputy Headteacher.
- Staff training in safe and responsible internet use, digital literacy and on the contents of this policy will be provided as required.
- A partnership approach with parents will be encouraged, with relevant information on issues covered by this policy made available.
- Cases of internet misuse and other disciplinary breaches related to the policy will be dealt with through the school's Behaviour, Bullying and Safeguarding/Child Protection Policies, as appropriate. In cases of potential radicalisation/extremism The Prevent Duty will be implemented and could involve referral of individuals to the Prevent Duty Delivery Board and the Channel Panel (after consultation with KSCB and Police).
- Any complaints associated with the application of this policy will be dealt with through the school's Complaints Procedure.