POLICY ON INTERNET USE AND E-SAFETY

Equal opportunities lie at the heart of all that we do at Silverwood School. We are committed to ensuring that every member of the school community is given the same chance as any other to access the services and support of the school

We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

This policy is designed to meet the needs of all pupils, working through pre-formal, semi-formal and formal curricula. It is inclusive of students who function at early/preverbal levels of language and communication, through to those who express themselves verbally and in writing. The policy is designed to be child-centered and to make sure as far as is possible that pupils understand what is happening in their lives, why, and what options are available to them

Approved by:	Resource Committee	Date:May 2025

Last reviewed on:	May 2025

Next review by:	May 2026

Co-operation – Respect – Perseverance – Kindness – Honesty – Courage

This policy should be read in conjunction with the following documents:

- Computing Curriculum;
- Personal Use of Social Media;
- Data Protection Policy;
- Lettings;
- Behaviour Policy,
- Safeguarding policy

RATIONALE FOR INTERNET USE IN SCHOOL

The internet is an essential element in 21st century 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.

The purpose of internet use in school is to raise educational standards, to promote student achievement, wellbeing and 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.

The internet poses additional risks to students. It is now part of our responsibility to ensure our students know how to be safe on the internet, now and in their future life.

ROLES AND RESPONSIBILITES:

THE ROLE OF THE DSL (Terri Chard)

- Co-ordinate the school's On line safety ethos, culture
- Ensure that staff follow the on line policy and
- Ensure the curriculum is fit for purpose and updated with current trends and technologies
- To support the Computing Lead to discharge their duties below
- To link online safety to all other relevant polices eg safeguarding, staff behaviours, appropriate use, staff behaviours.
- To be the lead contact for Securus (outsourced monitoring) for level 4 and 5 incidents.
- To follow safeguarding and DOFA protocol when dealing with on line incidents by either pupils or staff
- To sample network usage and logs;
- To approve access where requested to sites previously filtered;

THE ROLE OF THE COMPUTING CURRICULUM LEADER (Sarah Curwin)

- To help and support colleagues in the use and teaching of the internet through the curriculum;
- To ensure Responsible Internet Use and E-safety are covered in the relevant Computing teaching plans;
- To keep up-to-date with developments in internet and mobile technology;
- To organise and lead relevant in-service training and meetings.

THE ROLE OF Human Resources (Sarah Shepherd)

- To ensure that non-educational users of the school's internet are made aware of the policy on internet access;
- To support the DSL to coordinate a response to illegal and/or suspicious content that is discovered on the school's network;
- To ensure GDPR compliance.

THE ROLE OF THE INTERNET SERVICE PROVIDER (Oakford Internet Services)

- To provide a filtered Internet connection with a flexibility for school to make changes to the filtering rules as deemed necessary.
- To ensure the DSL and HR teams can access regular and on demand reports for internet usage
- To assist the school with the annual review of filtering & monitoring solutions
- To liaise with Securus (outsourced monitoring provider) to ensure the monitoring solution is operational.

1 HOW WILL INTERNET USE ENHANCE LEARNING?

1.1 The school internet usage is designed for educational use and includes filtering appropriate to the age of students;

1.2 Staff should guide students in online activities that will support the learning outcomes planned for the students' age, maturity and cognitive ability;

1.3 Students are taught appropriate internet use and are given clear objectives for internet use. They are taught how to use the internet for research, including the skills of knowledge location, retrieval and evaluation.

2 HOW INTERNET ACCESS IS AUTHORISED

2.1 Students are talked through a Responsible Internet Use Agreement at the start of each school year;

2.2 Parents are informed that students only have supervised internet access;

2.3 Community users of the school's IT facilities (e.g. for lettings, training and other non-educational activity) must confirm acceptance of the school's Acceptable Use Policy. In the case of lettings, appropriate wording will be included in the Letting's Booking Form. A copy of this policy will be made available to all other users.

3 MANAGING INTERNET FILTERING

3.1 The school works in partnership with parents, and Oakford Internet Services (OIS) to ensure systems to protect students are regularly reviewed and improved;

3.2 If staff or students discover unsuitable sites, the URL (address) and content must be reported by email to the Internet Service Provider (OIS) at support@oakfordis.com (the Director of Finance & Resources should be copied into any such notifications to track the response). Students must report to a member of staff and then the member of staff will ensure that it is reported.

3.3 Website logs are sampled and monitored by the Head of Campus and DSL;

3.4 The Computing Coordinator at each site will send regular reminders concerning Internet Safety to staff;

3.5 Any material that the school believes is illegal must be referred by a member of the Senior Leadership Team to Internet Watch Foundation;

3.6 Members of staff will be automatically provided with a separate set of filtering rules allowing less restrictive access to the Internet. The connection will still be filtered based on the underlying rules as set by the Internet Watch Foundation.

3.7 Any level 4 and 5 alerts that occur from the Securus Monitoring are investigated by DSL and logged with outcome.

4 MANAGING CONTENT

4.1 HOW WILL STUDENTS LEARN TO EVALUATE INTERNET CONTENT?

4.1.1 Specific lessons are included within the Computing curriculum plans that teaches appropriate students how to read for information from web resources. Where appropriate, students are taught to acknowledge the source of information used and to respect copyright when using internet material in their own work;

4.1.2 If staff or students discover unsuitable sites, the URL (address) and content must be reported via email to OIS at support@oakfordis.com" support@oakfordis.com. Students must report to a member of staff and the member of staff will ensure it is reported.

4.1.3 Schools should ensure that the use of internet derived materials by staff and by students complies with copyright law. Training is available to staff in the evaluation of web materials and methods of developing students' critical attitudes;

4.1.4 The Computing Coordinator will be responsible for recommending the permission of additional websites as requested by colleagues to leadership/ the Director of Finance & Resources for final instruction.

4.2 HOW SHOULD THE SCHOOL'S WEBSITE CONTENT BE MANAGED?

4.2.1 The point of contact on the website is the school address, school e-mail and telephone number. Staff or students' home information are never published;

4.2.2 Written permission from parents or carers will be obtained before photographs of students are published on the externally accessible sections of the school's website;

4.2.3 Website photographs that include students are selected carefully in line with the relevant permission being given and do not enable individual students to be clearly identified;

4.2.4 Students' full names should not be used anywhere on the website;

4.2.5 Where audio and video are included (e.g. Podcasts and Video Blogging) the nature of the items uploaded will not include content that allows the students to be identified.

5 COMMUNICATION

5.1 MANAGING STUDENTS' EMAIL (where appropriate)

5.1.1 Students may only use e-mail accounts at school which have been approved by the teacher taking the lesson;

5.1.2 Students must immediately tell a teacher if they receive offensive or suspicious e-mail. This information must then be passed to the Curriculum Coordinator who will notify the Oakford support desk (who are able to modify the settings to allow for some tracking of the message). This should always be supervised by a senior member of school staff.

5.1.3 Students must not reveal details of themselves or others in email communication, such as address or telephone number, or arrange to meet anyone;

5.1.4 Students should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly;

5.1.5 Access in school to external personal e-mail accounts may be blocked;

5.1.6 Social e-mail use can interfere with learning and is restricted;

5.1.7 E-mail sent to an external organisation should be written carefully, and must not be in breach of the Data Protection Act (1999);

5.1.8 Information is available to parents explaining how students can access their accounts from home.

5.2 ONLINE COMMUNICATIONS AND SOCIAL NETWORKING (where appropriate)

5.2.1 Students are taught about how to keep personal information safe when using online services. Each year group will have specific Computing lessons dedicated to e-safety;

5.2.2 The school conducts regular student and parent surveys about home use of ICT. The results gauge the range of activities which students undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.;

5.2.3 The use of online chat is not permitted in school, other than as part of its online learning environment;

5.2.4 Staff are permitted to use their phones to access the internet only when not with children and when they are on a break. This is predominantly used to access their school emails: see the Personal Use of Social Media policy.

6 MOBILE TECHNOLOGIES

6.1 Students' personal mobile phones are not permitted during the school day (subject to point 6.2). These are collected in at the start of the school day and returned during taxi time;

6.2 Appropriate use of mobile phones will be taught to students as part of their PSHE programme and within the KS4 Computing Scheme of Work;

6.3 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the Curriculum Coordinator and/or Director of Finance & Resources before use in school is allowed;

6.4 The sending of abusive or inappropriate text messages is forbidden. Any such activity will be followed up within the schools safeguarding and behaviour policy.

7 INTRODUCING THE E-SAFETY POLICY TO STUDENTS

7.1.1 Each year, a module on Responsible Internet Use and E-safety is included in the Computing curriculum covering both school and home use. This includes the necessity of keeping personal information safe, how to use mobile technologies and using online communication appropriately;

7.2 Students are informed that internet use is monitored;

7.3 The school uses relevant, up-to-date resources to teach and reinforce understanding about Responsible Internet Use and E-safety;

7.4 These messages will be followed by assemblies and tutor sessions on safeguarding issues;

7.5 Staff receive regular updates on E safety topics

7.6 Pupils learning is based around the 4 Cs of online Safety: Content, Contact, Conduct and commerce

8 PARENTS AND E-SAFETY

8.1 Parents' attention is regularly drawn to the School's E-Safety Policy in newsletters, and on the school Website;

8.2 Information will be available to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home. This is also signposted on the website;

8.3 There are parent support sessions offered to discuss internet safety topics.

9 STAFF AND THE E-SAFETY POLICY

9.1 All staff including teachers, supply staff, classroom assistants and support staff, are provided with the School Internet and E-Safety Policy and its importance explained;

9.2 The school's consequences for internet and mobile phone/PDA/technology misuse are clear in the annual safeguarding training along with the whistleblowing policy;

9.3 All staff will follow the terms of the 'Responsible Internet Use' statement before using any internet resource in school;

9.4 Staff are made aware that internet traffic is monitored and reported by OIS and can be traced to the individual user. Discretion and professional conduct is essential;

9.5 Staff development in Safe and Responsible Internet Use and on the school internet policy will be provided as required;

10 COMPLAINTS PROCEDURE

10.1 Responsibility for handling student IT-related incidents is delegated to the Senior Leadership Team;

10.2 Any complaint about staff IT misuse must be referred to the Head of Campus and DSL;

10.3 The school's Complaints Procedure is published on the website and in the school's policy;

10.4 The school works with parents and students need to work in partnership with staff to resolve issues;

10.5 There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies. In such cases, a Senior Leader is informed;

10.6 If students transgress then they will be offered support and advice on how not to repeat the action - parents and carers will be informed
If this is repeated then a removal of internet or computer access for a period, will be considered;

10.7 Sanctions available for staff include:

- Disciplinary action
- In the most severe cases, this could lead to dismissal.

11 POLICY REVIEW

Approved by: Senior Leadership Team Date: April 2025
Last reviewed on: May 2025
Next review due by: May 2026