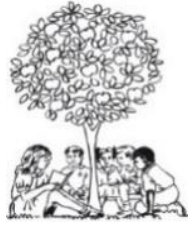


# The Orchard Infant School

## E-Safety Policy



### Policy Summary

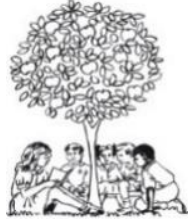
This policy outlines the roles, responsibilities and policies which relate to successful induction of Early Career Teachers

Document Detail		
Document Type		
Document Name	E-Safety Policy 2024	
Version	2	
Effective from	January 2024	
Review date due	January 2025	
Owner	The Orchard School	
Author	Sally Cary	
Approved by, date	18.1.24	
Superseded documents	E-Safety Policy 2023	
Related documents	Staff Acceptable Use of Technology Safeguarding and Child Protection Policy Taking, Storing and Using Images of Children Policy Complaints Policy	
Keywords		
Relevant external law, regulation, standards	<ul style="list-style-type: none"> <li>Data Protection Act 1998.</li> </ul>	
Supporting references		
Change History		
Date	Change details, since approval	Approved by
8.1.24	Filtering and Monitoring addition	
8.1.24	Addition of Projective Evolve Outline– online safety curriculum -	

E-Safety Policy 2024

Policy Version: 2

Approved Date: January 2024



**The Orchard Vision:** *Inspiring Success*  
**Values:** *Determination, Courage, Respect and Kindness*

## **The Orchard E-Safety Policy**

### **2024**

#### **Writing and reviewing the E-safety policy**

The E-safety Policy is reviewed as practice develops and relates to other policies including those for ICT, bullying and for child protection.

- The school has appointed an E-safety/ ICT team which include the DSL Leader, ICT technician, ICT subject leader and 2 other members of teaching staff.
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The E-safety Policy and its implementation will be reviewed annually.
- The E-safety Policy was revised by: Sally Cary

#### **Teaching and learning**

##### **Why Internet and digital communications are important**

- 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is provided by Surrey County through the Unicorn contract and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- 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 shown how to publish and present information appropriately to a wider audience.

##### **Pupils will be taught how to evaluate Internet content**

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- 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 be taught how to report unpleasant Internet content. Additional guidance is available via The Orchard Web Site, follow "Links" and view Thinkuknow.
- **'Bee Safe Monitor' is included on the pupil laptops to enable pupils to report concerns.**
- Through the Project Evolve Curriculum, children will be taught about the following areas of e-safety: Self-image and identity; Online Relationships; Online Reputation; Online

E-Safety Policy 2024

Policy Version: 2

Approved Date: January 2024

## **Managing Internet Access**

### **Information system security**

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

### **E-mail**

- Staff and pupils may only use approved e-mail accounts on the school system. Pupils have a school e-mail address to be used to access teams, they should be supervised when using this.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to pupil email communication must only take place from within Microsoft Teams and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

### **Published content and the school web site**

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

### **Publishing pupil's images and work**

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.
- Pupils' names will be not included on the Web site or blogs, forums or wikis, 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.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories (see the Taking, Storing and Using Images of Children Policy).

### **Social networking and personal publishing on the school Microsoft Teams**

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords. **Only** Microsoft Teams is used at The Orchard.
- Newsgroups will be blocked 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 must not place personal photos on any social network space provided in the school Microsoft Teams.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff should not use social media accounts outside of school in a way that could the school could be identified from. They should also take care when posting or replying in a way that could bring the school into disrepute.

### **Filtering:**

Our school use a filtering solution called Unicorn Cloud Filtering Service. This is a flexible, safe web filter designed specifically for schools and supplied by Surrey County Council. The solution is based on an industry-leading web safety engine called Smoothwall. Smoothwall constantly scans the school's internet traffic and categorises harmful materials. It prevents harmful material before it is displayed to the user in the form of a block screen warning. This enables the users to safely use the internet and provide logs for the designated safeguarding lead of what has been viewed, whose device and account information for monitoring purposes. In the event of harmful/inappropriate content being accessed, a block screen appears and informs them that the user cannot see the content of that webpage.

### **Monitoring:**

The Orchard also use an eSafety solution called BeeSafe. This software is developed by Beebug and provides monitoring of all staff and student workstations whether on-site or off-site using cloud-based technology. BeeSafe constantly monitors users keyboard input as well as screen output to detect harmful keywords typed or seen on the screen this includes swearing, sexual content and words linked with extremism and/or terrorism. If harmful content is detected a screenshot (or capture) is taken with the user's computer name, IP address, username and timestamp. Captures are reviewed by eye and are collated ad-hoc by Beebug who send the schools designated safeguarding lead and computing technician a weekly or monthly report for review depending on what has been captured and when.

### **Mobile Phones**

- Pupils will not bring or use mobile phones on the premises.
- Staff will ensure mobile phones are not used in classrooms or other child accessible areas (including Clubs). **They should remain within staff bags or staffroom lockers.**
- Mobile phone cameras will not be used within the school by staff to take pictures at any time.
- Staff will use a school phone where contact with parents is required.

### **Use of school technology outside of the school environment**

- The school may provide staff with technology for use in completing their jobs outside of the school environment. Staff should be aware that the same policies apply to these devices when used outside the school environment.
- Staff should not use these devices for any other purpose except that which is required to complete their professional work. Any staff found to be misusing school technology will have these devices removed from them and disciplinary action may be taken.

### **Protecting personal data**

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

### **Policy Decisions**

E-Safety Policy 2024

Policy Version: 2

Approved Date: January 2024

### **Authorising Internet access**

- All staff must read and sign the 'Staff Acceptable Use of Technology' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- **At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.**
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site.

### **Assessing risks**

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

### **Handling E-safety complaints**

- Complaints of Internet misuse will be dealt with by the Head Teacher or Assistant Head Teachers
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (please see the Complaints policy).
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

### **Community use of the Internet**

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

## **Communications Policy**

### **Introducing the E-safety policy to pupils**

- Appropriate elements of the E-safety policy will be shared with pupils
- E-safety rules will be posted in areas where laptops or other internet capable devices are.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

### **Staff and the E-safety policy**

- All staff will be given the School E-safety Policy and its importance explained.
- 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 senior management and have clear procedures for reporting issues.

E-Safety Policy 2024

Policy Version: 2

Approved Date: January 2024

### **Enlisting parents' support**

- Parents' and carers' attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-safety.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

### **E-Bullying (Cyberbullying)**

- E-bullying is the use of any communication medium to offend, threaten exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion.
- The school expects all members of the school community to communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by the school.

Updated: January 2024

# **The Orchard**

## **Staff, Governor and Visitor**

### **Acceptable Use of Technology / ICT Code of Conduct**

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school.

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

Any concerns or clarification should be discussed with Sally Carey, Head Teacher.

- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email / Internet / Intranet / Microsoft Teams and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.
- I will only use devices given by the school for professional purposes.
- I will ensure that I sign out any IT equipment owned by the school and ensure it is secure at all times when not in school.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without the permission of the ICT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network/Microsoft Teams without the permission of the parent/carers, member of staff or Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

E-Safety Policy 2024

Policy Version: 2

Approved Date: January 2024

- I will report any incidents of concern regarding children's safety to the E-safety Coordinator, the Child Protection Liaison Officer or Head teacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will ensure that pupils will not have access to my personal social networking sites.
- I will ensure that any posting or replying on personal social media accounts will not make reference to the school or be perceived as unprofessional.
- All staff will adhere to expectations of professional conduct and confidentiality when using email and social networking sites.
- I will support the school's E-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote E-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will not use my mobile phone within areas that children access during the school day, nor use the camera on my mobile for school purposes.

**User Signature**

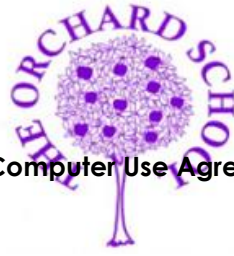
I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name.....(printed)

Job title.....

Signature..... Date.....





## Pupil Computer Use Agreement

When using computers at school I will:

- ask a teacher or suitable adult if I want to use the computers/tablets
- use technology safely, sensibly and respectfully
- use websites that I have been directed towards by my teacher
- not go on a website or download anything without permission from my teacher
- inform an adult if I see something that upsets me
- not give out any of my personal information online
- treat others kindly and respectfully
- ask for help or guidance if I need it
- have fun, enjoy my learning and stay safe

Signed Pupil .....


Date .....


Signed Parent .....


Date .....

### Children's E-Safety Rules

**Think then Click**  
These rules help us to stay safe on the Internet

 We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do. 

 We can search the Internet with an adult.

E-Safety Policy 2024

Policy Version: 2

Approved Date: January 2024

We always ask if we get lost on the Internet.



We can send and open emails together.

We can write polite and friendly emails to people that we know.



B. Stoneham & J. Barrett