# CHARLWOOD VILLAGE PRIMARY SCHOOL

# Online Safety Policy

| | |
|---|---|
| Policy Name | Online Safety Policy 2024-2025 |
| Policy Owner | Headteacher |
| Governing Body or Working Group Approval | Full Governing Body |
| Last Reviewed | Autumn 2024 |
| Next Review Date | Autumn 2025 |
| Status and Review | Statutory (KCSiE) and annually |

## Writing and Reviewing the Online Safeguarding Policy

The Online Safeguarding Policy relates to other policies including those for Computing, Anti-Bullying and Child Protection.

- Ms Luck is the Online Safeguarding Leader as the role overlaps with the Deputy Designated Safeguarding Lead and Computing Lead.
- Our Online Safeguarding Policy has been written building on best practice and government guidance. It has been agreed by all staff and approved by governors.
- The Online Safeguarding Policy and its implementation will be reviewed annually.

## 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 Internet provides a vast amount of information and for children to become effective citizens they must learn how to access information on the Internet
- The school Internet access is provided through School's Broadband provider 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 to report inappropriate Internet content to their teacher.

## 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 and implemented with the broadband provider and school IT support technician.

**E-mail**

- **Pupils and staff may only use approved e-mail accounts on the school system**.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone
- Staff to pupil email communication must only take place via a school email address and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Children will only e-mail external bodies when supervised by a member of the teaching staff.
- The forwarding of chain letters is not permitted.

**Published Content and the School Website**

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 Governors, staff or pupils personal information will not be published.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

**Publishing Pupil Images and Work**

- Photographs that include pupils will not include their names
- Pupils' full names will not be used on the Website
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website at the beginning of each school year
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

**Social Networking and Personal Publishing on the School Website**

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.
- 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 learning platform.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

**Managing Filtering**

- The school will work in partnership with Surrey County Council, internet provider School's Broadband and technician support from Soft Egg to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Designated Safeguarding Lead.

- The Computing Leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Soft Egg will send the school a report each month to show websites banned and any attempted accesses to banned sites.

**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 formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Staff may take their own mobile phones on educational trips to use to contact the school.
- Lessons may be filmed using a Flip Camera for monitoring the quality of teaching and learning. After using it as a discussion tool between the member of staff and the Headteacher the footage is deleted.
- Staff will use a school phone where contact with pupils is required.

**Protecting Personal Data**

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

**<u>Policy Decisions</u>**

**Authorising Internet Access**

- All staff must read and sign the 'Staff Code of Conduct' 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.**
- **In Key Stage 2, access to the internet will be by adult demonstration with direction to approved websites. Pupils will be provided with a unique log-in and password to monitor access.**
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school (e.g. Governors, Students, Soft Egg and Pre-School) will be asked to sign an Acceptable Use Policy 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.

**Handling Online Safeguarding Complaints**

- Complaints of Internet misuse will be dealt with by the Designated Safeguarding Lead.
- 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.
- Parents will be informed of the complaints procedure.
- 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 Online Safeguarding Policy.

**Communications Policy**

- Introduce the Online Safeguarding Policy to pupils
- Appropriate elements of the online safeguarding policy will be shared with pupils
- Online Safeguarding rules will be posted in classrooms.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of online safeguarding issues and how best to deal with them will be provided for pupils

**Staff and the Online Safeguarding Policy**

- All staff will be given the School Online Safeguarding Policy with the Staff Handbook at the start of the academic year and its importance will be 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 the Designated Safeguarding Lead and have clear procedures for reporting issues.

**Enlisting Parent Support**

- Parents' and carers attention will be drawn to the Online Safeguarding Policy on the school website.
- Parents and carers will from time to time be provided with additional information on online safeguarding.
- The school will ask all new parents to sign the Online Safeguarding Parental Consent Form when they register their child with the school.
- The Online Safeguarding Parental Consent Form will be sent annually at the start of the academic year. This will be monitored by the DSL and DDSL.

# Staff, Governor and Visitor Acceptable Use Agreement / ICT Code of Conduct

## Charlwood Village Primary School

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 Ms Lanham, Charlwood Village Primary School Designated Safeguarding Lead.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

- I understand that the school allows staff, governors, visitors to bring in personal mobile telephones devices for their own use. However, they must be kept away and may not be used in any part of the school where children will be.

- I will ensure when bringing personal devices into school that no inappropriate or illegal content is on the device.

- During class trips, adults will have access to their mobiles, which are to be used for emergency purposes only.

- 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 and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.

- 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 of software without the permission of the Head or Computing Leader

- 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/learning platform without the permission of the parent/carer, 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 the 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.

- I will report any incidents of concern regarding children's safety to the Designated Safeguarding Lead (Ms V Lanham) or Deputy Lead (Mr Tim Warren)

- 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 support the school's Online Safeguarding Policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote online safeguarding with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.

**User Signature**

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

Full Name……(printed)

Job title……

Signature…… Date……

## Online Safeguarding Rules

Key Stage 1

# 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.

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.

Key Stage 2

# Think then Click

These rules help us to stay safe on the Internet

We ask permission before using the Internet.

We only use websites that an adult has chosen.

We immediately close any webpage we not sure about.

We tell an adult if we see anything we are uncomfortable with.

We only e-mail people an adult has approved.

We do not open e-mails sent by anyone we don't know.

We send e-mails that are polite and friendly.

We never give out personal information or passwords.

We never arrange to meet anyone we don't know.

We do not use Internet chat rooms or social media sites.

# Online Safeguarding Parental Consent Form

## Charlwood Village Primary School

## Parent/Carer Consent Form and Online Safeguarding Rules

**All pupils use computer facilities, including Internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that the Online Safeguarding Rules have been understood and agreed.**

**Parent / Carer name: ……**

**Pupil name: …….**

As the parent or legal guardian of the above pupil, I have read and understood the attached school Online Safeguarding Rules and grant permission for my daughter or son to have access to use the Internet, school email system and other IT facilities at school.

I know that my child has been made aware of online safety and that they have a copy of the school Online Safeguarding Rules. My child agrees to follow the Online Safeguarding Rules and to support the safe and responsible use of IT at Charlwood Village Primary School.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching online safeguarding skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their online safety or online behaviour that they will contact me.

I understand that given permission to walk home alone in Upper KS2, my child may bring a mobile phone device into school, hand it into the office at the start of the day and collect it at the end.

I understand that use of smart watches in school is strictly prohibited.

I understand the school is not liable for any damages arising from my child's use of the Internet facilities.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

**Parent/Guardian signature: ……..**

**Date: ……**
Further information for parents on online safeguarding can be found at the Think U Know website, Parent Zone or NSPCC.
**Please complete, sign and return to the School Office.**