WYKE PRIMARY SCHOOL

E-SAFETY POLICY

Formally adopted by the Board of Governors on October 29th 2017, for review October 2018

Our Nominated Governor for Safeguarding is

Sarah Snook

Our Designated Safeguarding Lead is

Olivia Palmer

Our Deputy Safeguarding Lead is

Claire Murphy

Wyke Primary School E-Safety Policy

The school has identified a member of staff who has an overview of E-Safety (Emma Knott), who works closely with the school's DSL (Olivia Palmer). 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 the school's Governors.

The E-Safety policy

- Will be reviewed annually
- Discussed with staff
- Discussed with the school council and E-Safety group.

Teaching and Learning

- The Internet is an essential element of the 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 part of the curriculum and a necessary tool for staff and pupils
- The school Internet access is provided by Dorset County Council and includes filtering appropriate to the age of the pupils
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use (as in the children's Acceptable Use Policy)
- Pupils will be educated in the effective use of the Internet
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Evaluating Internet Content

- The school will seek to ensure that the use of Internet derived materials by staff and pupils complies with copyright law
- Pupils will 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.

Security

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

Internet Access

- All Internet activity should be appropriate to staff professional activities or the children's education
- Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person
- The Internet may be accessed by staff and children throughout their hours in school
- Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited

- Use for personal financial gain, gambling, political purposes or advertising is excluded
- Copyright of materials must be respected.

Email

- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive e-mail and a hard copy will be requested
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet with anyone without specific permission
- Staff to pupil email communication may only take place via a school email address
- Incoming email 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
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media
- Posting anonymous messages and forwarding chain letters is not acceptable
- The use of the Internet, e-mail, or any other media to access inappropriate materials such as pornography, racist or any other offensive material is forbidden.

Social Networking Sites

- Staff are not to discuss pupils, staff, parents or school matters associated with Wyke Primary via Social Networking sites. Any incidents will be reported to the Headteacher and logged
- It is strongly recommended that Staff are not linked to Parents of pupils at Wyke Primary School via social networking sites.

Internet Publishing Statement

The school wishes the school's web site to reflect the diversity of activities, individuals and education that can be found at Wyke Primary School. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles will be borne in mind:

- No video recording may be published without parental consent of the child concerned, and the child's own verbal consent.
- Surnames of children should not be published, without parental consent, especially in conjunction with photographic or video material

- No link should be made between an individual and any home address (including simply street names)
- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in doubt, refer to the person responsible for child protection
- All staff members are responsible for the material published to the school website.

Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the nominated member of staff and reported on the online safety incident log
- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Other devices

- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity and by staff only if permission has been authorised by the Headteacher
- The sending of abusive, offensive or inappropriate material is forbidden
- Staff should not share personal telephone numbers with pupils and parents
- Staff should be aware of the potential uses of information technology for bullying and abusive behaviour between young people
- Staff should be aware of 'sexting' and understand their duty to report any concerns.

Tapestry

- Staff should log out of the Tapestry app or program when they are finished in order to maintain confidentiality
- Staff should not share log in or password details with any person not employed by Wyke Primary School
- Staff should not share any information or photographs relating to children with any person not employed by Wyke Primary School
- Staff should take all responsible steps to ensure the safe keeping of any portable device e.g. tablet that they are using and report any missing devices
- If accessing Tapestry with a private computer, not on school premises, staff must maintain confidentiality and professionalism
- All entries on Tapestry must be appropriate
- All entries on Tapestry remain the property of Wyke Primary School
- At all times staff must comply with Child Protection policies and E-Safety policies.

Authorising Internet use

- All staff must read and sign the Acceptable Use Agreement Policy

- All pupils must agree to sign and comply with the E-Safety Home-School agreement, before being granted Internet access.

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. The school cannot 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 appropriate and effective
- The school will monitor pupil's use of the internet during lessons in accordance with 'The Prevent Duty Guidance' relating to the Counter-Terrorism and Security Act 2015 that came into effect on July 1st. (See Safeguarding Policy Section 10- Radicalisation and Extremism).

Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of Staff and recorded on the '**Online Safety Incident Report Sheet'.** (Located in the staff room)
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be referred to the Designated Safeguarding Lead (Olivia Palmer). And dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of consequences for pupils misusing the Internet
- All use of the school Internet connection by The Red Heron Club and any other after school clubs/organisations shall be in accordance with the E-Safety 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 all networked rooms
- 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
- All staff will read, understand and sign the Staff Acceptable Use Policy

- Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Parent support

- Parents and carers attention will be drawn to the school E-Safety Policy in newsletters and on the school website
- Parents will be provided with information on acceptable use of the Internet through their E-Safety Home-School agreement
- The school will ask all new parents to sign the E-Safety Home-School agreement when they register their child with the school.