That they may have life; life in all its fullness - John 10:10

Hordle CE (VA) Primary School

E-SAFETY POLICY 2021

Any reference to 'the school' throughout this policy shall mean Hordle CE (VA) Primary School and Nursery.

Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy should operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and IT Security policies. It should also be read in conjunction with the Staff Acceptable use of ICT policy. It is also a key element of the school's PREVENT Duty and trained staff have considered this policy and its links to anti-radicalisation of all types.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering systems
- The adherence to the Data Protection Policy and the General Data Protection Regulations ("GDPR") when using any device that can send and receive information within and outside the Hordle domain for both staff and children

1.0 School e-safety policy

1.1 Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT and for child protection.

- The school's e-Safety Lead is also the ICT Coordinator. They will work in close co-operation with the Headteacher and deputy heads and the safeguarding team which includes governors. The e-safety lead will liaise with the Designated Safeguarding Leads.

- Our e-Safety Policy has been written by the school. It has been agreed by the staff and governors.

1.2 Teaching and learning.

1.2.1 Why Internet use is 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.

1.2.3 Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught what Internet use is acceptable and what is not. This will include what to do in the event that inappropriate/unsuitable material is seen. They will be given clear objectives for Internet use.

- Internet access will be planned to enrich and extend learning activities, particularly in KS2 where it is a core strand of the curriculum.

- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content will be reported to the Headteacher.

- Staff should 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.

1.2.5 Pupils will have frequent e-safety sessions

- Each half term will commence with the first computing lesson being an e-safety session. These will follow the published curriculum and help support the children in being safe online both in and out of school.

- Children in UKS2 will receive more regular e-safety training which will focus on social media usage in particular as this will help to prepare them for its use once they are of the appropriate age (Majority of social media apps/sites are 13+). As part of the UJs e-safety curriculum they are taught modules from Year 7 and 8 to help better prepare them for a future online.

1.3 Managing Internet Access

1.3.1 Information system security

- The school's information management systems are secured by Hampshire County Council
- Locally, virus protection will be installed and updated regularly.
- The school uses broadband with appropriate firewall and filters as recommended by HCC.

1.3.2 E-mail

- Pupils may only use approved e-mail accounts (@hordleprimary.co.uk) on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Children's email accounts have filters in place to identify certain words, phrases and abbreviations. These emails are redirected to the SLT so that they can be dealt with appropriately.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff e-mails sent to an external organisation should be written carefully, with reference to all relevant policies including the Data Protection Policy and the GDPR.
- The forwarding of chain letters is not permitted.

1.3.3 Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The governors will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Published content must adhere to the school Data Protection Policy, please contact the Data Protection Officer for more information or if unsure how to proceed.

1.3.4 Publishing pupil's images and work

- Pupils' full names will not be used anywhere online, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published online, including for the school website, blog and Tapestry.
- When publishing pupil's images and work, staff must adhere to the school Data Protection Policy. Please contact the Data Protection Officer for more information or if unsure how to proceed.

1.3.5 Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved. (Facebook and other social media will be unblocked during E-Safety training at the beginning of the year so that certain settings can be demonstrated.)
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school is likely to be inappropriate for primary aged pupils. This information is communicated through bulletins in the newsletter, e-safety workshops and e-safety leaflets.

1.3.6 Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.

1.3.7 Managing videoconferencing (COVID amended- Jan 2021)

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- External IP addresses should not be made available to other sites.
- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing should be supervised appropriately for the pupils' age and conform to the Data Protection Policy.

1.3.8 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 (With the exception of the Headteacher's device, see 1.6 Use of the Headteacher's personal device for more information).

The sending of abusive or inappropriate messages is forbidden, regardless of app/site/operating system.

- Staff have access to a school phone where contact with parents/pupils is required.

1.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the GDPR.
- All staff will adhere to the school Data Protection Policy to keep personal data protected, please contact the Data Protection Officer for more information or if unsure how to proceed.

1.4 Policy Decisions

1.4.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff, including Governors, Teaching Assistants and Supply Teachers must read and sign the acceptable ICT Acceptable Use of ICT Policy before using any school ICT resource.

1.4.2 Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of 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 governors / Headteacher will monitor compliance with the e-Safety Policy.

1.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the headteacher.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures by the head teacher/Designated Safeguard Lead.
- Pupils and parents will be informed of the complaints procedure.
- Sanctions may include: – interview/counselling by class teacher / headteacher; – informing parents or carers; – removal of Internet or computer access for a period.

1.4.4 Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- It would not ordinarily be expected that parents would be given use of school ICT equipment. If there is cause to do so, this decision should be made in conjunction with the headteacher.

1.5 Communications Policy

- **1.5.1 Introducing the e-safety policy to pupils**
- Advice for pupils will be posted in all classrooms.
- Pupils will be informed that Internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.

1.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained. The use of social media and how to use the security/safeguarding features will be refreshed during INSET day health and safety training at the beginning of the year.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

1.5.3 Enlisting parents' / carers' support

- Parents' / carers' attention will be drawn to the School e-Safety Policy in newsletters.

1.6 Use head teacher's personal device

- The chair of governors has given the head teacher express permission to her personal device in her role as head teacher within the school. This enables her to record photographs, notes and commentary during observations and learning walks as part of the performance management process and to provide evidence and/or feedback.
- The Headteacher's device will be used in line with the Data Protection Policy and the GDPR.
- The Headteacher's device will be secured using the features available through their operating system to the highest possible level, e.g. passcode, fingerprint scan, eye scan etc.
- To ensure transparency the head teacher will surrender her personal device to the chair of governors upon her request.

This policy was reviewed by the Governing Body in the year:	2021
This policy is scheduled for review in the year:	2022