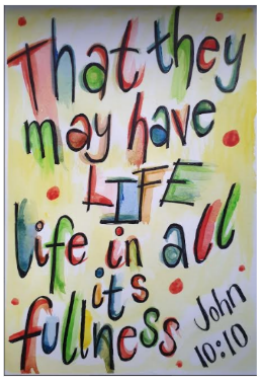
That they may have life; life in all its fullness - John 10:10

Hordle CE (VA) Primary School & Nursery

E-SAFETY POLICY 2023

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

Through an education rooted in God's love and grounded in our community through teamship, our children will shape their identity to become aspirational learners, with enquiring minds and deeply held personal values ready to take on their responsibilities; living life in all its fullness as Global Citizens of the future.



Contents

1. 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.

This E-Safety Policy outlines our commitment to promoting safe internet use amongst our pupils and provides guidance for both students and staff. The school's e-safety policy should operate in conjunction with other policies including the Behaviour and Relationships Policy, the Anti-Bullying Policy and those on safeguarding, the curriculum, data protection and IT security. 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.

2. Aims and Objectives

Our primary aims and objectives with regard to internet safety are as follows:

1. To ensure the safety and well-being of our students while they are using the internet both within the school premises and at home.
2. To educate our students about the potential risks and responsible use of the internet.
3. To provide guidance to teachers and parents on internet safety.
4. To establish clear procedures for addressing internet safety incidents.
5. To continually review and update our internet safety practices to reflect the evolving nature of online technologies and threats.

3. Roles and Responsibilities

3.1 Students:

1. Students are expected to use the internet in a responsible and respectful manner, following the guidelines provided in this policy.
2. They should not share personal information, such as their full name, address, phone number, or school details, with anyone they meet online.
3. Students must report any inappropriate or harmful online content or behaviour to a trusted adult, such as a teacher or parents

3.2 Teachers:

1. Teachers are responsible for supervising and guiding students in safe internet use during school hours.
2. They should incorporate age-appropriate internet safety education into the curriculum.
3. Teachers should be vigilant in identifying any concerning online behaviour among students and take appropriate action.
4. The school's E-Safety lead is also the Computing Lead and will work in close co-operation with the Headteacher, Deputy Head and the Safeguarding Team which includes governors.

3.3 Parents/Guardians:

1. Parents and guardians are encouraged to be actively involved in their child's online activities and set appropriate limits on screen time.
2. They should educate their children about online safety and monitor their internet use at home.
3. Parents are urged to report any concerns or incidents related to internet safety to the school so that home and school can work in partnership.

4. Internet Safety Education

We will provide regular internet safety education to students, including topics such as:

1. Recognising and avoiding online risks, such as cyberbullying, inappropriate content, and online scams.
2. Protecting personal information and privacy online.
3. Responsible social media and online communication.
4. The importance of reporting any online concerns to a trusted adult.

5. Internet Filtering and Monitoring

We will implement appropriate internet filtering and monitoring systems to block access to inappropriate content and to ensure that students are using the internet safely while at school. Filtering reports will be checked regularly by the Lead DSL and acted upon to ensure compliance with this policy.

No internet filtering is 100% effective and on accidentally discovering material that makes them feel uncomfortable we instruct students to:

1. Calmly switch off their screen without showing their neighbours.
2. Tell a teacher, trusted adult or member of staff straight away.

6. Incident Reporting and Response

Any incidents related to internet safety will be taken seriously and addressed promptly. Our response may include:

1. Investigating the incident.
2. Involving parents/guardians and, if necessary, the appropriate authorities.
3. Implementing appropriate consequences for students involved in harmful online behaviour.
4. Offering support and guidance to victims of online harassment or bullying.

7. 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 GDPR (as defined in the Data Protection Policy) when using any device that can send and receive information within and outside the Hordle domain for both staff and children

8. Teaching and Learning

8.1 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.

8.2 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.

Staff will be aware of the web-filtering and monitoring systems in place to safeguard pupils.

8.3 Pupils Will Be Taught How to Evaluate Internet Content

If staff or pupils discover unsuitable sites, the URL (address), time, date and nature of content will be automatically sent to the Web Filtering and Monitoring inbox;

Pupils will also be actively taught, through E-safety lessons, to report any unsuitable content and the URL, time, date and nature will be submitted by a staff member using the 'E-safety Report Form'. This will then be referred to the Web Filtering team for blocking.

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.

Staff will vigilantly monitor pupils' devices whilst accessing the internet.

8.4 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 further 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.

9. Managing Internet Access

9.1 Information System Security

The school's information management systems are secured by Harrap ICT. Locally, virus protection is installed, updated regularly and managed on all devices by Harrap ICT.

The filtering is based on categories provided and updated by the IWF (Internet Watch Foundation).

The school uses broadband with appropriate firewall and filters as recommended by Harrap ICT.

9.2 E-Mail

Pupils may only use approved email accounts (@hordleprimary.co.uk) on the school system. Children are not allowed access to personal email accounts or chat rooms whilst in school.

Pupils must immediately tell a teacher if they receive an offensive email and are taught to retain the email as evidence to share with a trusted adult.

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 email communication, or arrange to meet anyone without specific permission.

Staff emails 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.

9.3 Published Content and the School Website

The contact details on the website should be the school address, email 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.

9.4 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 Online Learning Diary.

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.

9.5 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 explicitly taught 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, email 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.

9.6 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 Headteacher and the E-Safety coordinator.

The school will adhere to the guidance in KCSIE around web-filtering and monitoring duties.

9.7 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 section 11.4, Use of the Headteacher's personal device for more information). Staff may, in exceptional circumstances, use mobile phones with express permission from the headteacher with completion of consent form. Once authorised, Photographs taken as part of a lesson will be uploaded to school secure network and deleted from staff member's device, witnessed by headteacher or SLT member

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.

9.8 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.

10. Policy Decisions
10.1 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.

10.2 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, in line with web filtering and monitoring guidance, 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 despite the WatchGuard filtering systems in place. 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.

10.3 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 headteacher.

Complaints of a child protection nature will be dealt with in accordance with school child protection procedures by the Headteacher/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.

10.4 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.

11. Communications Policy

11.1 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.

11.2 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.

11.3 Enlisting Parents/Carers Support

Parents' / carers' attention will be drawn to the School e-Safety Policy in newsletters, along with regular featured articles on current considerations/risks surrounding eSafety.

11.4 Use of Head Teacher's Personal Device

The chair of governors has given the headteacher express permission to use 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.

12. Review and Update

This Internet Safety Policy will be reviewed annually by the governing body and revised as needed to ensure its effectiveness and relevance.

By implementing this policy, we aim to create a safe and secure online learning environment that empowers our students to make responsible choices while using the internet.

	DATE	Ethos	Equality	Practice	Guidance
This policy was reviewed and screened by the Governing Body	2023	☑	☑	☑	☑
Next scheduled review:	2024	☐	☐	☐	☐