HAREWOOD

Educating For 'Life In All Its Fullness'

Harewood C of E Primary School

Internet Safety Policy

(Previously E-Safety Policy)

Date Approved: Spring 2025

Chair of Governors: J. Jayne

Headteacher: A. Ratcliffe

Date for Review: Spring 2028

School Ethos and Values

Educating For 'life In All Its Fullness'

(John 10:10)

As a school, we shape what we do, to allow children and adults to develop a strong sense of their Emotional, Spiritual and Cultural self through our Christian values:

We actively work towards our children being prepared for life as active citizens in the communities and world they live in.

<u>Safeguarding</u>

The Governing Body and staff of Harewood C of E Primary School take as our first priority the responsibility to safeguard and promote the welfare of our pupils, to minimise risk and to work together with other agencies to ensure rigorous arrangements are in place within our school to identify, assess, and support those children who are suffering harm and to keep them safe and secure whilst in our care.

<u>Equal Opportunities</u>

We have a clear duty under the Equality Act 2010 to ensure that our teaching is accessible to all pupils. Our inclusive curriculum will foster good relations between pupils, tackle all types of prejudice, including racism and homophobia, and promote understanding, tolerance and respect, enabling us to meet the requirements, and live the intended spirit, of the Equality Act 2010.

E-Safety Policy

The policy is written in line with the 4C's (Content, Contact, Conduct, and Commerce) as stated in the Keeping Children Safe in Education 2024 Document: **https://www.gov.uk/government/publications/keeping-children-safe-in-edu…**

Staff with specific e-safety roles and responsibilities

E-Safety Lead	Alistair Ratcliffe
DSLs	Alistair Ratcliffe Jen Flowerdew
All adults working in school have a responsibility to safeguard the children, other adults and school resources in relation to e-safety and online responsibilities	

Our e-Safety Policy has been written by the school, building on the Leeds e-Safety Policy and government guidance. It has been agreed by all staff and approved by governors

Teaching and learning

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. Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. This is currently provided by EXA NETWORKS using the Surf-Protect filtering system.

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 taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with the law.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

- The school has a single server which is split virtually into s separate systems, the admin (office) and curriculum (rest of school). These are connected but staff will only be able to access SIMs as well as their own content.
- The head teacher and Business Manager are the only staff to be able to access both networks from one computer.
- The school has a secure wireless network which links with the curriculum server.

Wireless Network

- The schools wireless network is secure. There is a password which only the computing subject leader and ICT technician know.
- Pupil devices (iPads and laptops provided by school) are already set up on the network.
- Staff are advised to contact the computing leader when accessing with personal equipment.
- It will be managed by the computing subject leader / e-safety coordinator and ICT technicians.

How will the staff & children be made aware of this policy and be taught about using the internet safely and respectfully?

- Children will cover modules of internet use/safety as part of the PSHE and Computing Curriculum. (See individual curriculum progression maps for coverage)
- Children in Year 3 will also be made specifically aware of the 'Rules for using ICT' document - where in they will sign and agree to follow code of conduct it describes. This will be refreshed at the start of each year in KS2.

E-mail

- Pupils from Year 3 onwards may be setup an Office 365 account but only be given access to this once appropriate teaching and rules have been put in place. This includes the children signing a usage agreement.
- Pupils may only use approved e-mail accounts on the school system.
- 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.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- 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 headteacher takes overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Only pupils' forenames will be used on the Web site, especially in association with photographs.
- Pupil's work can only be published with the permission of the parents (List of non-authorised children has been created for every year group and is shared with staff).
- All parents / carers will need to give consent before their child(ren)s photographs or videos will appear on the website.

Social networking and personal publishing

- EXA NETWORKS will block/filter access to social networking sites.
- Sites 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 and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and as part of staff training on online safety.

Managing filtering

The school will work with the Surf-Protect (through exa-networks) to ensure systems to protect pupils are reviewed and improved. Surf-Protect can be accessed by SchoolsICT technical support.

If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator, or supervising adult, who will look into it and add into the restricted section in the filtering system.

Managing videoconferencing

- Video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

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. The sending of abusive or inappropriate text messages is forbidden.
- Staff will use a school phone where contact with pupils or parents is required. If a school phone is unavailable (for example, the staff member is working from home), the private number must be blocked before dialling.

Protecting personal data

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

Policy Decisions Authorising Internet access

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2, there will be times where more open use of the internet is required to support learning. This will be only with the consent and supervision of a responsible adult.

Assessing risks

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. Neither the school nor Leeds City Council can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the e-safety coordinator.
- 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 where required.

- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Community wider use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety. Cyberbullying
- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- Incidents of cyberbullying reported to the school will be recorded in the same way as other behaviour related incidents.
- There are procedures in place to investigate incidents or allegations of Cyberbullying and this will be in accordance with the schools anti-bullying policy.

Communications Policy Introducing the e-safety policy to pupils

E-safety rules will be discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored.

Pupils will have an Online Safety Day, using UK Safer Internet resources linked with National Online Safety resources and will have workshops annually delivered by D:Side.

Staff and the e-Safety policy

All staff will be given access to 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.

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters, at parental meetings and on the school Web site. For more information on supporting children online please visit: **https://parentzone.org.uk/** and the school website **https://harewood.leeds.sch.uk/online-safety/**

Addendum 1 – Taken from SAFEGUARDING & CHILD PROTECTION POLICY FOR SCHOOLS & COLLEGES

Children and online safety away from school

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.

Online teaching should follow the same principles as set out in the Guidance for safer working practice for those working with children and young people in education settings (National Safer Recruitment Consortium May 2019).

School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

School staff may choose to deliver live classes during and school closure. Short video recordings may be produced and published on the school website for children and parents to view e.g. reading a story. A range of platforms may be used to engage children in these, including Microsoft Teams, Zoom and Tapestry.

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- No 1:1s, groups only.
- In cases where 1:1 tuition is essential, staff must seek formal agreement from a senior manager and the pupil's parent.
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; staff need to be mindful that backgrounds do not compromise personal confidentiality or breach the guiding principles of safer working practice guidance for staff working in educational settings.
- The live class will be recorded where possible, so that if any issues were to arise, the video can be reviewed. Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background. Staff must only use platforms specified by senior managers and approved by our IT network manager / provider to communicate with pupils.

Cyberbullying

School has a responsibility for its children's welfare whether they are in school or out of school, especially when it comes to technology. The school's procedures, when it comes to Cyberbullying, reflect the schools Anti-bullying policy when investigating incidents or allegations of Cyberbullying.

We will investigate reports of Cyberbullying fully, looking into both sides where possible. Appropriate action will be taken. Parents / Carers will also be informed. We will let the person who was Cyberbullied know what happened and a discussion between the two may happen.

We will teach people all about Cyberbullying and how to help young people support each other. We will teach people all about Cyberbullying and how to help young people support each other and investigate as much details as we can find out. We will let the person who was Cyberbullied know what happened, how far it has been investigated. Teach the person how to deal with this situation, should it happen again.

Other Policies and Guidance which should be read in conjunction with this policy include:

- Safeguarding and Child Protection Policy
- LCC guidance for Staff working in Educational Settings on the Use of Digital Technologies and Social Media
- On line Safety Guidance for schools
- Acceptable usage policy
- Photograph permission forms
- Rules for using ICT staff/pupils
- Social Media Policy
- Mobile Phone Policy
- Safer Working Practices (Including guidance on Remote Education)