Hermitage

Internet Safety Policy 2021-2022

Hermitage Primary School			
Review frequency	Annually	**Reviewed**	January 2022
Governing Committee Responsible		**Governor Approval (date)**	
Website	Yes		
Staff Responsible (Head teacher)	Elaine D'Souza	**Next Review**	January 2023

1) Importance and benefit of the Internet in schools:

- The purpose of Internet use in schools is to raise educational standards, to promote pupil achievement, to support the professional work of staff and pupils and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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 so that they can gain insight into world-wide resources.
- Staff can develop their professional skills through access to national developments, educational materials and good curriculum practice.

2) How will pupils act online and learn about using the Internet?

- Pupils will understand the SMART rules when using the Internet. (Safe, Meeting, Accepting, Reliable, Tell)
- Pupils in Early Years will begin learning about Internet Safety through the Smartie the Penguin programme. Pupils will hear the story of Smartie the Penguin and answer associated questions throughout the story to help Smartie make the best decisions whilst on the internet. Pupils will learn a simple safety message in the form of a song, which will be repeated on several occasions.
- Pupils in Years 1 – 6 will be taught structured Internet Safety lessons from the PIXL programme. There are separate schemes for Years 1 and 2, Years 3 and 4 and Years 5 and 6.
- Ensure they are aware of the risks involved with using the Internet and changes that are occurring.

- Pupils must immediately tell a trusted adult if they receive anything offensive online. They should also keep the e-mail until the trusted adult can take evidence of the material.
- Will not deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- Should use language that is sensible and appropriate. Language which is used to bully or be rude to someone will not be acceptable.
- Should only contact and arrange to meet people they know or those the teacher has approved.
- Pupils must keep personal details to themselves. These can include: where they go to school, their home address(es), telephone numbers, passwords.
- Pupils have Internet Safety lessons at the start of the academic year and refer to them throughout the year.

3) How staff will ensure best practice:

- Training will be given to staff in the evaluation of web materials.
- Ensure they are aware of the risks involved with using the Internet and changes that are occurring.
- Take time to understand and read the policies and procedures put into place, as well as Internet Safety material they may receive.
- Internet safety will be explicitly taught to the pupils**.**
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Carry out ½ termly Internet Safety focused sessions with the pupils they work with.
- Inform pupils that their Internet use is monitored.
- Ensure that all web-based content shared with pupils during whole class teaching is age appropriate.
- Access to the Internet will be demonstrated by an adult, with directly supervised access to specific, approved on-line materials.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider (LGfL) via the Computing Co-ordinator or Headteacher.
- Report all Internet Safety issues immediately but not exceeding 24 hours of being alerted to the issue.
- E-mails 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.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Sign up and use the resources provided by National Online Safety.

4) How the school will ensure best practice:

- Promote the positive use and values of the Internet, including use of Social Media.
- Educate those within the school about Internet Safety and what to do if that safety is compromised.

- Have a clear procedure for flagging Internet Safety related issues (use CPOMS and send to the Headteacher and SLT).
- Take all Internet Safety allegations seriously and deal with them promptly.
- Provide ½ termly materials for pupils and staff on Internet Safety related issues.
- Rules for Internet Safety will be posted in all rooms where computers are used.
- Take part in national events, such as, Internet Safety Day.

5) How will school online accounts be managed?

- Website photographs that include pupils will be selected carefully.
- Only first names of children will be used online.
- Photograph permission will be sought from parents/carers via a consent form.
- Teachers will be made aware of those who have not consented to photos.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

6) How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to the Headteacher or a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Any complaints against the Headteacher must be raised with the Chair of the Governing Body.

7) How will we protect ourselves against cyber crime?

Cyber crime is criminal activity committed using computers and/or the internet. It can involve malicious attacks on computer software, including:

Email hacking
Email hackers try to gain access to email accounts by tricking people to:

- open and respond to spam emails
- open emails with a virus
- open phishing emails

Phishing
Phishing messages look authentic with corporate logos and a similar format to official emails.
Sometimes phishing emails use the title of a genuine email that the victim has recently replied to in order to trick the victim into believing the communication is authentic.
Phishing emails can appear to have originated from within or outside your organisation.
Unlike official communications, phishing emails ask for verification of personal information, such as account numbers, passwords or date of birth.
Sometimes the emails suggest the request is time sensitive to pressure the recipient to respond when they might not otherwise have done so.

Unsuspecting victims who respond may suffer stolen accounts, financial loss and identify theft.

Malvertising
Malvertising can compromise computers by downloading malicious code when people hover on or click on what looks like an advert. Some will even download malicious code to your computer while the website is still loading in the background. Cyber criminals can use advertisements as a way to hack into computers.

To address the risk of fraud, theft and/or irregularity, we:

- use firewalls, antivirus software and strong passwords
- routinely back up data and restrict devices that are used to access

We also train staff to ensure that they:

- check the sender of an email is genuine before, for example, sending payment, data or passwords
- make direct contact with the sender (without using the reply function) where the email, for example, requests a payment or change of bank details
- if telephoning the sender to confirm authenticity, do not use the contact number within the email without first checking it is genuine
- understand the risks of using public Wi-Fi
- understand the risks of not following payment checks and measures

This is not an exhaustive list.

Signed____
Date__________________

Chair of Governors

Signed____
Date__________________

Headteacher