WHITEHILLS PRIMARY SCHOOL

"…putting children first…."

E-SAFETY POLICY

Date reviewed: **January 2022**

Reviewed by: **N James**

Ratified by Governors: **January 2022**

The importance of E-Safety

Computing in the 21st century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Pupils use the Internet widely outside of school and will need to learn how to evaluate Internet information and to take care of their own safety and security. Consequently, at Whitehills we need to incorporate these technologies in order to give our children the skills they need to access lifelong learning and employment. E-Safety involves pupils, staff, governors and parents making best use of technology, information and training to create and maintain a safe on-line and computing environment at Whitehills.

Provision

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. As such, the school has a duty to provide pupils with quality Internet access as part of their learning experiences:

- The school Internet access will be appropriate for pupils, as it will have appropriate content filtering.
- Pupils will be given clear advice upon Internet use and taught what use is acceptable and what is not.
- Pupils will be taught how to use the Internet effectively for research, including the skills of knowledge location, retrieval and evaluation.
- As part of the current computing curriculum all year groups will cover various elements relating to staying safe on line. For example password security, digital footprints and cyber bullying.
- The school will ensure that the use of materials from the Internet will comply with copyright law.

Pupils are taught to evaluate the information they obtain from the Internet and check its accuracy carefully.

Reporting

All breaches of the e-safety policy need to be reported on MyConcern. The details of the user, date and incident should be reported. Incidents which may lead to child protection issues need to be passed to one of the Designated Safeguarding Leads immediately – it is their responsibility to decide on appropriate action not the class teachers. Incidents which are not child protection issues but may require intervention (e.g cyberbullying) should be reported to the E-safety lead and the Head teacher promptly.

Allegations involving staff should be reported to the Head Teacher. If the allegation is one of abuse then it should be handled according to the DFE document entitled ‘dealing with allegations of abuse against teachers and other staff’. If necessary, the LADO (Local Authorities Designated Officer) should be informed.

Evidence of incidents must be retained.

The curriculum will cover how pupils should report incidents.

Protecting Personal Data

Personal data shall be recorded, processed, transferred and made available in accordance with current legislation.

Assessing Risk

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 does not accept liability for the material accessed, or any consequences of Internet access. The school will audit use to establish whether the e-safety policy works appropriately.

Handling E-Safety Complaints

- A senior member of staff will deal with complaints of Internet misuse.
- Any complaint of misuse of the Internet by staff must be reported to the Headteacher.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Whilst computing is exciting and beneficial in and out of education, web based resources are not well policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. Also, their individual responsibilities relating to the safeguarding of children and themselves, in school and at home.

Educating pupils about the dangers of technologies that may be encountered outside of school will be done in an informal manner through the E-Safety curriculum.

Pupils are aware of the impact of cyber bullying and know how to seek help if they are affected by any form of online bullying.

Managing the Internet

- The school maintains that pupils will have supervised access to Internet resources. All staff will preview any recommended sites before use.
- Raw images searches are discouraged when working with pupils. If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents supervise their children whilst using the Internet.

Authorised Internet access

- All staff must read and sign the 'Acceptable Use Agreement' before using any school computing resource.
- Parents will be informed that pupils will be provided with supervised Internet access..
- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework and sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an e-safety log, which will be stored in the Headteacher's office with other safeguarding materials.
- The school will 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 are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

Internet Use

- Pupils at Whitehills are too young to use social networking sites, such as Facebook (the legal age limit is 13 years old). However, we recognise children are accessing the sites at home and provide information about ensuring privacy levels are high and that children are aware of the risks.
- Annual E-safety reminders are taught – specifically in E-Safety week (February) but also each term through the National Online Safety hub we subscribe to.

Security and Passwords
Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always ‘lock’ the PC if they are going to leave it unattended.

Password security

- Password security is essential for pupils.
- Pupils are expected to keep their passwords secret and not share with others, particularly their friends.
- Staff and pupils are regularly reminded of the need for password security.

Software security

- A security breach, lost/stolen equipment, virus notification, unsolicited emails and all other policy noncompliance must be reported to senior management.
- To minimise risk, pupils should not bring homework to school using portable memory sticks.

Information System Security

- School computing systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- E-Safety will be discussed with our computing support and those arrangements incorporated into our agreement with them.

Remote Access
The school provides access to some areas of the school network remotely. This allows staff to login to the school network from outside school to retrieve documents and files. Files and documents are unable to be downloaded or printed. Remote access to school systems is restricted to those specified staff who need access and removed immediately when a staff member leaves the school. Staff accessing the school’s computing facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant and take such precautions as the IT support, Headteacher and E-safety lead may require. Passwords for remote access will be complexed in nature, have a 100-day expiration, a 30 password history (a password cannot be reused if used within the last 30 passwords) and a 10 failed attempts lockout.

EQUAL OPPORTUNITIES
All children should have equal access to remote learning in order to develop their personal capabilities.

Resources are checked to ensure that gender and ethnicity are reflected in a balanced way without stereotyping.

The co-ordinator, in conjunction with the SENCO, will advise teachers on support that can be provided to children with particular individual needs.

The co-ordinator will also advise teachers on how to develop e-safety awareness for all abilities.

INCLUSION
Teachers ensure that the work undertaken by children with a disability: takes account of their pace of learning and the equipment /resources they use; takes account of the effort and concentration needed. We ensure that any child who needs to learn remotely has access to appropriate hardware and software.

E-mail

- Staff should only use their school email when sending professional emails.
- Staff should use password protected emails / Switch Egress when the content is of a sensitive nature.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

- Pupils must immediately tell a teacher/trusted adult if they receive and offensive email.
- Pupils are introduced to e-mail as part of the computing curriculum.
- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety.
- Pupils must not reveal personal information about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Chain letters, spam, advertising and all other e-mails from unknown sources will be deleted without opening or forwarding.

Social Networking

- Use of social networking sites and newsgroups in the school is not allowed and will be blocked/filtered.
- Pupils will be advised to never give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Mobile Phones

Most new mobile phones have access to the internet and picture and video messaging. Whilst these are great developments for technology, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils are allowed to bring mobile phones to school as long as they are handed in to their teacher at the start of the school day and parents have completed a mobile phone disclaimer.
- Pupils are not allowed to use their mobile devices once on the school site.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use the school phone to contact parents.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom.
- Staff may have their mobile phones on their person to use in an emergency on playtime and lunchtime duties or whilst outside when there is outdoor PE lessons.
- All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.
- Parents cannot use mobile phones on school trips to take pictures of the children.
- On trips staff mobiles will be carried and may be used for emergency only.

Roles and Responsibilities

Headteacher and Senior Leads:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibilities for e-safety will be delegated to the e-safety co-ordinator.
- The Headteacher/Senior Leaders are responsible for ensuring that the e-safety coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.

- The Headteacher and Deputy should be aware of the procedures to be followed in the event of a serious e-safety allegations being made against a member of staff.

The E-Safety Lead

- Takes day-to-day responsibility for e-safety and has a leading role in establishing and reviewing the school's e-safety policy/documents.
- Liaises with the school computing technical staff.
- Support other staff with e-safety issues.

Communication of Policy

Pupils:

- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites such as Instagram and Facebook. This will be strongly reinforced across all year groups during computing lessons and all year groups will look at different areas of safety.

Staff:

- All staff have access to the school e-safety policy and its importance explained annually.

Parents:

- Parents' attention will be drawn to the school e-safety policy in newsletters, through Parentmail, the school's newsletters and on the school website.

Further Resources

We have found these web sites useful for e-safety advice and information.

http://www.thinkuknow.co.uk

Set up by the Police with lots of information for parents and staff including a place to report abuse.

http://www.childnet-int.org

Non-profit organization working with others to "help make the Internet a great and safe place.

Policy revised - January 2022

Appendix 1

Acceptable Use Policy – Staff
Completed annually September

Note: All internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both, you must sign this policy sheet.

Internet Access – You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-Safety Officer (Sarah Mitchell) and an incident sheet completed.

Social Networking – is allowed in school in accordance with the e-Safety Policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks.

Use of Email – Staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the *Data Protection Act.*

Passwords – All staff have personal passwords for laptops, MyConcern etc. Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support. Shared passwords, e.g. Google Calendar, are to be changed by the Headteacher and/or the school office team only.

Remote Access – You must keep all login and password details for remote access secure, never saved or stored on any device outside school and always logout completely when the remote access session has finished. Staff must take all reasonable precautions to ensure remote access sessions are secure.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive, etc.) is encrypted. On no occasion should data concerning personal information be taken off site on an unencrypted device.

Personal Use of School computing equipment – You are not permitted to use computing equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos – You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal computing equipment– Use of personal computing equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment. A risk assessment will be carried out by IT support and the e-Safety Officer.

Viruses and Other Malware – Any virus outbreaks are to be reported to the e-Safety Officer and Headteacher as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Purchasing Apps/Software – This must be in agreement with the e-Safety Officer and ICT co-ordinator to ensure validity and safety for students.

e-Safety – Like health and safety, e-safety is the responsibility of everyone to everyone. As such, you will promote positive e-safety messages in all use of computing whether you are with other members of staff or with students.

e-Safety concerns must be logged on MyConcern.

I understand that any breach of the policy may lead to disciplinary action.
NAME:

SIGNATURE: **DATE:**

Appendix 2

Acceptable Use Policy – Students Years 4-6
Our Charter of Good Online Behaviour
Completed annually (February)

Note: All internet and email activity is subject to monitoring

I promise – to only use the school computing equipment for schoolwork that the teacher has asked me to do.

I promise – not to look for or show other people things that may be upsetting.

I will not – use other people's work, pictures or photos without permission to do so.

I will not – damage the equipment. If I accidently damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames and passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will not – sign up to sites or apps inappropriate for my age.

I will not – bring to school my mobile phone without prior permission from the Headteacher.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online. I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent): **Print:**

Signed (Student): **Print:**

Date: