SHEERHATCH PRIMARY SCHOOL

ACCEPTABLE USE & E-SAFETY POLICY 2019

At Sheerhatch Primary School we believe in the many benefits of technology including the use of the internet and that pupils need the skills and understanding to navigate this virtual world effectively and safely. The internet is also a vast source of teaching resources and as such is regularly used by teachers in both the planning and delivery of lessons as well as by administration staff and school leadership in a number of management systems.
This policy sets out the procedures in place to keep everyone safe from potential harm that may arise from irresponsible or malicious use of the internet.

SCHOOL NETWORK

The school's computer network is managed by Partnership Education who review and test the security systems regularly.

The school reserves the right to check **ALL** user data including temporary Internet files and history files.

Our Broadband services are provided by Schools Broadband (Talk Straight) who employ a filtering system designed specifically for schools. Hence the uploading and downloading of non-approved application software is denied to pupils. New application software is only loaded on to the school system by our technician from Partnership Education with permission from the Head Teacher.

All access to the school network requires entry of a recognised User ID and password. Pupils have limited access on pupil specific User IDs and should sign out or shut down after every session.

Virus protection software is installed and updated regularly through Partnership. Staff are encouraged to use email or the google drive to transfer documents and data in order to reduce virus infections of laptops and the school's network.

CLASSROOM MANAGEMENT

Pupils only use PCs, laptops or tablets in supervised activities and are monitored by the teacher or other adults.

Pupil and teacher login accounts ensure that individuals receive the appropriate home pages and access rights.

Laptops are positioned in such a way that they are easily observed by teachers.

Our Internet codes of conduct are shared and agreed with all parents/carers and pupils and are displayed in class rooms and around the school.

USE OF THE INTERNET

Electronic information skills are now fundamental in the society our pupils live in. Access to the Internet opens up classrooms to a vast array of resources and enables pupils to explore thousands of libraries, databases and bulletin boards and the possibility to exchange messages with people throughout the world. The school therefore encourages the pupils to use the rich information resources available on the Internet, together with the development of appropriate skills to analyse and evaluate them.

The staff are encouraged to use the Internet as a teaching resource and to blend the use of such information as appropriate within the curriculum. Staff will consult the Computing Coordinator for advice on content, training and appropriate teaching levels consistent with the school's Computing programme of study. When using the Internet with pupils, staff will provide guidance and instruction and they will reference E-safety in their lesson planning.

Unfortunately, because internet access may lead to any publicly available site in the world, pupils may access electronic information resources which have not been selected by teachers as appropriate for use by pupils. Whilst our aim for internet use is to further educational goals and objectives and school procedures will be followed along with a strict network filtering system, it is possible that pupils may find ways to access other materials as well. The school believes that the benefits to pupils from access to information resources and increased opportunities for collaboration exceed the disadvantages. Ultimately however, parents and guardians are responsible for setting and conveying appropriate standards that their children should follow when using media and information sources. All parents/carers are given an Internet Code of Conduct to sign. (See appendices)

Guidelines for Internet use

All students are taught effective online research techniques, including the use of search engines. Receiving information over the web or in e-mail or text messages presupposes good information-handling skills:

- Using alternative sources of information for comparison purposes.
- Using search technologies effectively, appreciate how results are selected and ranked and be discerning in evaluating digital content.
- Identifying an author's name, date of revision of the materials, and possible other links to the site.
- Respecting copyright and intellectual property rights.
- Adding a url link underneath images downloaded from the internet.
- Referencing websites used for research.
- Knowing a range of ways to report concerns and inappropriate behaviour.

Staff may review files and communications to ensure users are using the system responsibly. Users should not expect that files and e-mails stored on servers will always be private.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear responsibility for such guidance as they must exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

***The following are not permitted*:**

- Sending or displaying offensive messages or pictures.
- Using obscene language.
- Harassing, insulting or attacking others-cyberbullying.
- Damaging computers, computer systems or networks.
- Violating copyright laws.
- Intentionally wasting limited resources.

E-SAFETY

Online safety school contacts

Any online safety issues involving pupils, either inside or outside of school, will be handled sensitively by the Designated Safeguarding Leads (Helen Ryan, Danica Kipling and Louise Buisson) and parents/carers informed when necessary. A record of the incident will be kept on My Concern.

Cyberbullying

Cyberbullying is the use of technology to bully a person or group. Cyberbullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot easily defend him or herself. The victim of cyberbullying does not have to own an electronic device themselves to be cyberbullied.

Children can cyberbully each other in a number of ways including:

- Sending abusive texts and emails.
- Posting/sharing hurtful messages, images or videos.
- Imitating others online.
- Excluding others online.
- Nasty online gossip and chat.

The school views cyberbullying like any other form of bullying. Reports of cyberbullying will be dealt with swiftly by a member of SLT. If a pupil reports an incident of bullying using e-mail or mobile phones, then they will be advised not to reply to the message. Evidence will be secured and preserved if possible. Parents/carers of both parties will be informed and given advice on how to deal with cyberbullying. An SLT member will speak to the class/classes of pupils involved about how to behave using electronic forms of communication. They will also speak separately to the pupils involved explaining that cyberbullying is not acceptable and enforcing the guidelines given to pupils in the Internet Code of Conduct and discussed during E-safety week. Steps will be taken to repair harm and to prevent recurrence.

If malicious or threatening comments are posted online about pupils or staff the school will inform the site administrator and request its removal. If deemed necessary, evidence will be sent to www.ceop.gov.uk/contact_us.html

The school will also consider informing the police depending on the severity and repetitious nature of the offence.

Abusive texts and phone calls

Malicious, abusive or threatening calls or texts are illegal. Pupils are taught to report incidences of unwanted text messages to a trusted adult either at home or in school. Pupils are told not to respond to any bullying messages and they should take a screenshot of these messages as proof. They should then report the incident to an SLT member at school. They

can also block the caller on their phone or contact their mobile phone provider directly-all UK operators have a nuisance or malicious call team, who can provide assistance. The pupil does not need to know the person responsible for making the call. A guidelines poster is displayed throughout the school. (Appendix F)

Internet Access

The school provides Internet access for educational purposes and it should only be used by staff, pupils and members of the school community for these purposes.

The school takes and will continue to take all reasonable precautions to ensure that students access appropriate material only. The school uses Schools Broadband as the Internet Provider. They are specialists in school internet and have a high level of filtering service. However, it is not possible to guarantee that a student will never come across unsuitable material while using a school networked computer.

Where reasonably possible, all Internet access by pupils is supervised by a member of staff or other responsible adult.

No pupil, member of staff or school community user is permitted to access material that is illegal or potentially offensive using school systems.

Students are made fully aware of the risks to which they may be exposed while on the Internet. They will be shown how to recognise and avoid the negative areas of the Internet such as pornography, violence, racism and exploitation of children.

However, if they encounter such material they will know that they should or close their laptop, minimise a screen on a PC or press their i-Pad home button, and then report the incident to the nearest teacher/adult who will deal with it according to the school policy. They will immediately report the details of any inappropriate or illegal Internet material found to the Internet Provider.

The school's website and social media

The school has its own website as well as Facebook and Twitter accounts. Ultimate responsibility for the content of the website and Social Media platforms rests with the Head Teacher in line with the following guidelines:

- The school is registered under the Data Protection Act.
- Individual pupils will not be identifiable by name.
- Names will not be linked to photographs or individual e-mail addresses.
- No personal information will be published without the individual's permission.
- Parental/carer consent will be sought prior to any reference (text, audio or photographic) to a child or children being published.

The copyright of all material produced by the school for display on the school's web pages belongs to the school. Permission to reproduce any other material will be sought and obtained from the copyright owner.

The contact details for the school will include only the school's postal address, e-mail address and telephone number. No information about teachers' home addresses or the like will be published.

Moderated email, newsgroups and chat rooms

Teachers will moderate other collaboration tools such as blogs, newsgroups etc., if used on the school network for learning purposes. Students will be denied access to public or un-moderated chat rooms. Only newsgroups that have educational goals and content will be made available to students.

All staff have a school linked e-mail address provided by gmail. Gmail provides encryption and secure email systems. **Staff must not use their personal e-mail details for school business.** Passwords of staff who have left will be changed immediately or deleted when no longer used.

ACCEPTABLE USE OF EQUIPMENT

Staff

When using IT equipment staff will follow the guidance and instructions given by relevant training and documentation relating to the specific equipment. Where members of staff are unsure of how to use equipment guidance must be sort from an appropriately trained member of staff.

Where IT equipment is taken off site the member of staff responsible must take every reasonable care to ensure that the equipment is looked after carefully (and locked out of sight in accordance with insurance policy). All hardware is asset tagged upon arrival in school. All serial numbers of hardware used by staff off site are recorded by the Finance Officer for insurance purposes.

Staff owned mobile phones **must not** be accessed or used during school hours with the exception of in the Staff Room. Mobile phones must be kept out of sight of pupils either in a classroom cupboard out of reach of pupils or in the lockers provided. The use of personal social networking sites in school is only permitted during break times and never in the presence of pupils.

Pupils

When using IT equipment pupils will follow the guidelines given by class teachers and will not purposefully handle the equipment in any way that might cause damage. **ALL** equipment will be used with the knowledge and guidance of a member of staff and shall be used to support learning.

Some older pupils from Y4 to Y6 may bring a mobile phone into school, if they have parental permission for good reason, such as that they walk home alone. All phones must be turned off and handed in to the class teacher, first thing in the morning, to be kept securely. Phones must not be accessed during the school day. Phones will be distributed before the child leaves school.

COMMUNICATING THE SCHOOL'S ACCEPTABLE USE POLICY (AUP)

Informing pupils

'Our Internet Code of Conduct' rules are displayed in all classrooms. (Appendix B). Pupils are aware that their Internet use is monitored and they are given rules on safe and responsible use of the Internet, Staying Safe on the Internet posters are displayed around the school (Appendix C). Pupils and their parents/carers must sign (Appendix D) before pupils are allowed to access the school network. Posters displaying guidelines to follow when pupils receive upsetting texts are also on display around the school. (Appendix E)

Informing staff

All staff will have access to a copy of the school's AUP. Staff are aware that Internet traffic can be monitored and traced to an individual user. Staff will be consulted regularly about the development of the school's AUP and instructions on safe and responsible Internet use. Staff will also sign the relevant part of the AUP document. Sections of the AUP are referenced in the staff Code of Conduct received by staff, students and volunteers at their induction.

To avoid misunderstandings staff will contact the Computing Coordinator regarding any doubts that arise concerning the legitimacy of any given instance of Internet use.

Informing parents/carers

Parents/carers attention will be drawn to the School's AUP on the website and by letter in the school starter packs. Advice that accords with acceptable and responsible Internet use by pupils at home will be made available to parents/carers.

The school obtains parental/carer consent before publication of students' work or photographs

Review

This Policy will be reviewed on an annual basis. The Policy was approved by the Governing Body at its meeting on:

Signed by Head Teacher ……

Signed by Chair of Governors ……..