HESWALL PRIMARY SCHOOL

E-SAFETY POLICY

E Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

This policy was adopted by the Governing Body on 18.11.20

This policy is due for review on 18.11.21

Heswall Primary School's E-safety Policy operates in conjunction with other policies including those for Pupil Behaviour, Anti-Bullying, Curriculum, Data Protection and Security.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; 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 from the Wirral Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications

Heswall Primary School acknowledges the assistant of Sheffield Children and Young People's Directorate and Kent County Council in providing content in this document.

E-Safety Audit

This quick self-audit helps the senior management team (SMT) to assess whether the e-safety basics are in place.

Has the school an E-Safety Policy that complies with CYPD guidance?	Y ~~/ N~~
Date of latest update: September 2020	
The policy was agreed by governors in: September 2020	
The policy is available for staff in Staffroom Policies file	
And for parents www.heswall-primary.wirral.sch.uk	
The designated Child Protection Teacher/Officer is: The Headteacher	
The E-Safety Co-ordinator is: the Headteacher	
Has E-safety training been provided for both pupils and staff?	Y ~~/ N~~
Is the Think U Know training being considered?	Y ~~/ N~~
Do all staff sign an ICT Code of Conduct on appointment?	Y ~~/ N~~
Do parents sign and return an agreement that their child will comply with the school's E-Safety Rules?	Y ~~/ N~~
Have school E-Safety Rules been set for pupils?	Y ~~/ N~~
Are these Rules displayed in all rooms with computers?	Y ~~/ N~~
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access	Y ~~/ N~~
Has the school filtering policy been approved by SMT/LA?	Y ~~/ N~~
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y ~~/ N~~

HESWALL PRIMARY SCHOOL E-SAFETY POLICY

Heswall Primary School has appointed the Headteacher as E-Safety Co-ordinator, in addition to his role as Child Protection Officer.

Our E-Safety Policy has been written using Government guidance.

The E-Safety Policy will be reviewed annually. This policy will next be reviewed in September 2021.

Why is Internet Use Important?

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Heswall Primary School has a duty to provide pupils with quality internet access.

Pupils will use the internet outside school and will need to learn how to evaluate internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils world-wide;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the LA and DCSF;
- Access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning:

- The school internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not, and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities;
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturing.

- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- Heswall Primary School will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the Internet Acceptable Use Policy before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the LA helpdesk via the headteacher/deputy headteacher or via network manager.
- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Unit to be taught in school.
- 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.
- Whole class or group e-mail addresses should be used in school.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations 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.

Social Networking

- Access to social networking sites and newsgroups are blocked/filtered via Wirral intranet.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and passwords set where appropriate, to deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others (see social networking policy).

Sexting

Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages.

They can be sent using mobiles, tablets, smartphones, laptops - any device that allows you to share media and messages.

Sexting may also be called:

- trading nudes
- dirties
- pic for pic.

What the Law Says

'Sexting can be seen as harmless, but creating or sharing explicit images of a child is illegal, even if the person doing it is a child. A young person is breaking the law if they:

- take an explicit photo or video of themselves or a friend
- share an explicit image or video of a child, even if it's shared between children of the same age
- Possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created. [Source NSPCC Sexting Guidance]'

Informing Children

- Sexting – Children in Year 5 and 6 will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the World Wide Web.

The School's Use of Social Media (Twitter/Facebook/Instagram):

The aim of this use of a Social Networking Site is to provide parents with effective and regular updates about what is happening at school and improve communication. The school will never contact any children (including past and present pupils) using social media and will not respond to any children's posts. The school will never use children's names. The school will only use images/videos with parental permission. The school will also constantly check the Twitter/Facebook/Instagram accounts, including followers, to ensure that any inappropriate users (due to content or inappropriate language used) are immediately removed/ blocked and reported. Social Media is not an acceptable way to communicate complaints/grievances and staff will not engage in resolution on Social Media sites. It is acceptable to advise people to follow the correct procedures and contact the school directly.

Filtering

Heswall Primary School has a service level agreement with Wirral IT Services as part of the Local Authority. The Authority regularly receives a file update to ensure that the firewall remains up to date with all new recognised threats and indecent/ inappropriate sites filtered and therefore inaccessible on any of the schools computer and network.

Video Conferencing

- IP 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 video conferencing call
- Video conferencing will be appropriately supervised for 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 for personal use during lessons or formal school time. The sending of abusive or inappropriate messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required, and also use their mobile to contact school if on a school trip.

Published Content and the School Website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified without parental permission.
- Pupils' full names will not be used anywhere on the website or blog, particularly in association with photographs
- Permission from parents/carers will be obtained before photographs of pupils are published on the school website.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LA.

Protecting Personal Data

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

Assessing Risks

- Heswall Primary 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. Neither the school nor the LA can accept liability for the material accessed, or any consequences of internet access.
- The school should audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety Policy is appropriate.

Handling E-Safety Complaints.

- Complaints of internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the headteacher.
- 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.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms;
- Pupils will be informed that internet use will be monitored.

Staff

- All staff will be given the school's E-Safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual use. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the school's E-Safety Policy in newsletters, and on the school website.

Prevent

At Heswall Primary, we must ensure that children are safe from terrorist and extremist material when accessing the internet in school and we therefore ensure that suitable filtering is in place. It is also important that we teach pupils about online safety generally.

The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions continues to be judged carefully.

Mobile Phones:

1. Pupils' mobile phones to be locked securely in Y6 lockers or handed in at the main school office.
2. Staff/Volunteers/Visitors not to use personal mobile phones apart from in the staffroom.
3. Staff to switch off the blue tooth on their mobile phone whilst in school.
4. No images of children to be taken on personal mobile phones.

Tablets/Cameras

The use of tablets and cameras may be used to record pictures of children's work, pictures of children for evidence of work and for recording special events. The photographs must not be published on newsletters, websites, Twitter or in any other media without the consent of the children's parents. If these devices are taken out of the school e.g. on a school trip they must be password protected. Any downloads of images/videos from tablets/cameras must not be on personal computers. Where downloads are stored on school computers, the computer must be password protected and must not be accessible on shared files.

Flash Drives

Flash drives that contain sensitive information [reports, photographs for learning journeys in F2, SEND information etc.] and are used by staff in their professional roles must be encrypted if they are to leave the site. Encrypted flash drives have been distributed to staff. Staff must not store files with sensitive information on their home computers. Back-up copies of encrypted flash drives containing sensitive information must be on password protected computers.

Clouds

Images/Videos of children must not be saved on personal clouds. If it is necessary to save images using web based applications then the use of Google Drive/Photos attached to each member of staff email must be used. Staff must ensure that personal devices (e.g. mobile phones personal computers) outside of school are not left unprotected without a password to ensure no third party can access school emails or other documents e.g. Google Drive or Shared Drive.

Cellular Data and Smart Watches

Children will not use cellular data e.g. 3g/4g/5g to connect any school devices. All internet connections will be through the school Wi-Fi so that the school filter is active. Typical devices using cellular data include mobile phones or tablets. Watches (such as smart watches) that use the internet to receive messages (text, e-mails voice), play games, record sounds, take photographs or make calls are not permitted to be worn/brought to school by children. Staff must not use personal smart watches to access these features when working with children.

Use of Google Classroom

Due to the increase in requirement of Remote Learning, the school utilises Google Classroom as part of G-Suite for Education. All accounts are strongly password protected. Where staff have access to Google Classroom, the classroom must be logged out before the computer is utilised by another person. This applies to staff accessing the platform both in the workplace or working offsite.

Children accessing the platform do so after communication to parents. The classrooms are by invite only and are consistently checked by classroom teachers and SLT. Staff may utilise Google Classrooms for both homework and remote learning. Children are advised of clear rules of use for the Google Classroom including the communication streams.

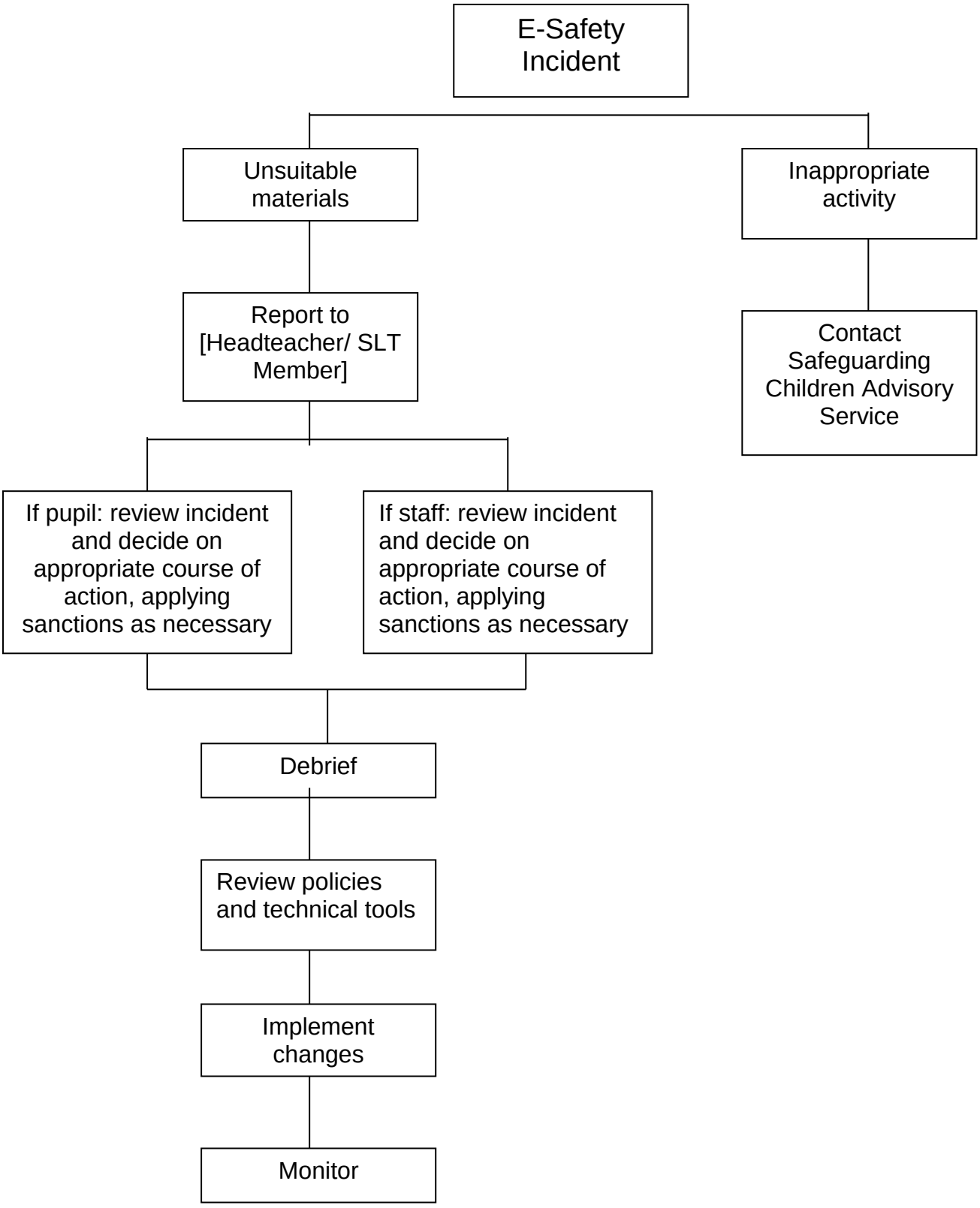
Staff may record suitable short videos to help children learn e.g. demonstration of a calculation etc. or read suitable stories to the children. Staff must be follow the same code of conduct when working online as when in the physical classroom. Google Classroom has the facilities for online class meet ups or for teacher giving instructions in the case where a whole class is not in school e.g. isolation due to the Covid-19 pandemic. Only the password protected Google Classrooms can be used to do this. Staff may only utilise these facilities with children when using official G-Suite for Education that is set up on their school email account.

Video Conferencing

Staff are able to utilise video conferencing facilities in school to liaise with other professionals and agencies. They may also contact other classes within the school. Where physical assemblies cannot take place, a secure video conference call can be used e.g. Google Meet/ Microsoft Teams (School has both securely set up). Children must not use the video conferencing applications unless it is under the guidance of a member of staff. When children are talking to other agencies e.g. social workers they may need more privacy yet supervision will still be required although the member of staff may supervise from a safe distance.

Appendix A

Flowchart for responding to E-Safety Incidents in School



HESWALL PRIMARY SCHOOL

COMPUTER AND PERSONAL INTERNET SAFETY

GUIDELINES FOR PARENTS

Although our children are young, many are entering school ICT literate. To protect them from the Internet and bulletin boards which contain explicit and unsuitable material, parents need to find out how control systems can be applied, and form their own household rules.

- Keep the computer in a family room rather than in a child's bedroom;
- Stay in touch with what your children are doing by spending time with them whilst they are on-line;
- Make 'on-line' a family activity;
- Make sure you know the services your child uses;
- Make on-line activities fun. Talk about the tasks and investigate further opportunities that would interest your child;
- Learn how to access the services – ask your child to explain the services to you;
- Be aware of school ICT activities and the school internet rules [see website – newsletter page];
- Go on-line yourself so that you are familiar with and understand the potential benefits and risks;
- Should you become aware of the presence of child pornography on-line, immediately report this to the NSPCC on 0800 800 500;
- Post your 'Family Internet Rules' near the computer as a constant reminder.

FAMILY INTERNET RULES

1. Always keep to the agreed times of day to be on-line and the length of time to be on-line;
2. Agree sites and areas that can be visited;
3. Never give any passwords to anyone outside the family – even friends;
4. Never give any personal information during a session;
5. Only visit 'chat' sessions when parents are working alongside children;
6. Always tell a parent about any threatening or bad language used.

KS1 Rules

These rules help us to stay safe on the Internet

Think then Click



We only use the Internet when an adult is with us.



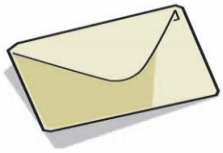
We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.



We always ask if we get lost on the Internet.



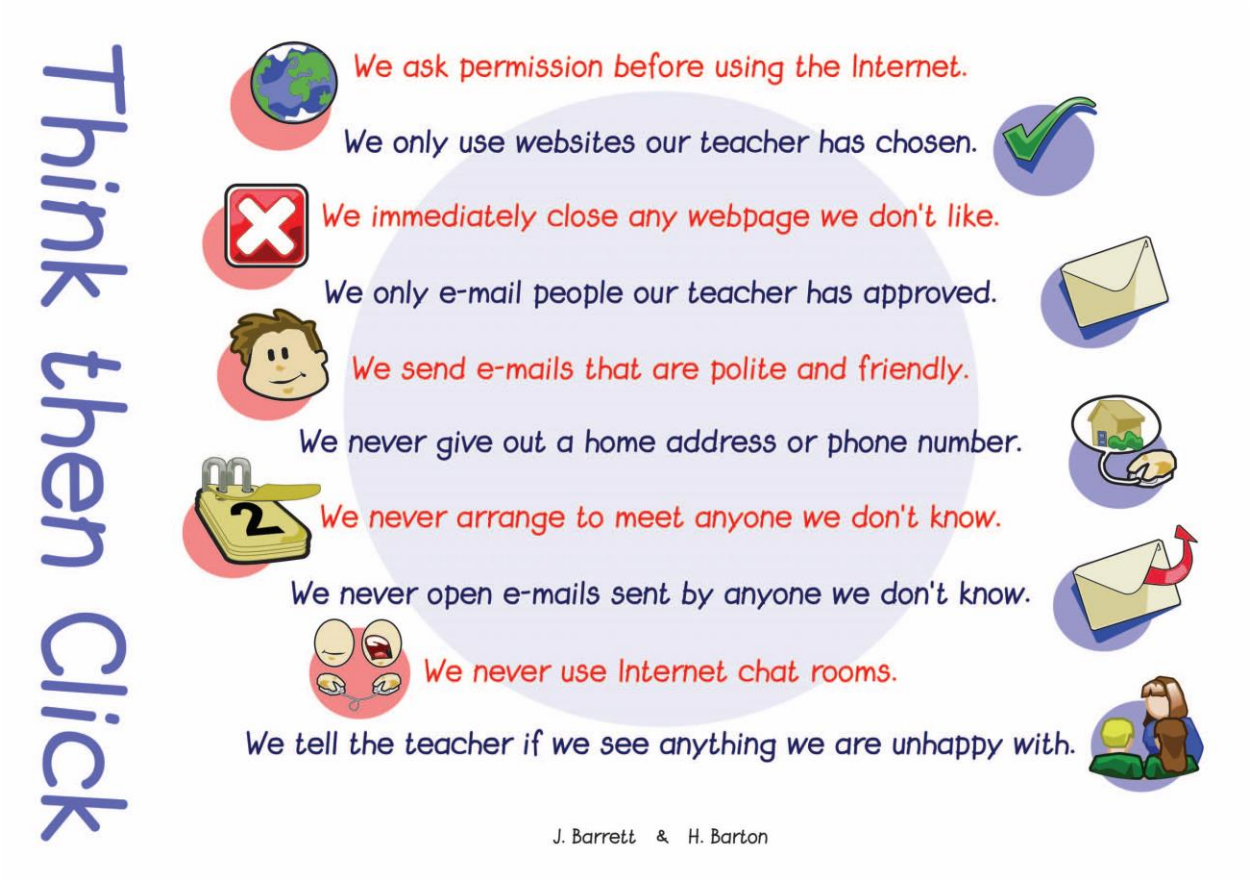
We can send and open emails together.



We can write polite and friendly emails to people that we know.

KS2 Rules

These rules help us to stay safe
on the Internet.



HESWALL PRIMARY SCHOOL

USE OF COMPUTERS AND THE INTERNET IN SCHOOL

Child's Name _____

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum and the Early Years Foundation Stage. Parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Access to modern technology including computers is an important part of our children's education. In our Reception class, children use the computer/tablet to learn their way around a computer screen and manipulate a mouse. They access programmes provided for them by staff, and there is very limited access to the Internet.

Heswall Primary School gains access to the Internet through a filter designed to block objectionable material. All children have supervised access to the internet.

As the parent, legal guardian or carer of the above named pupil, I acknowledge that my son/daughter will have supervised access to networked computer services and the Internet.

I understand that some materials on the Internet may be objectionable, but I accept that the school will do everything within its power to prevent my child from accessing such materials.

I also accept my responsibility for making it clear to my son/daughter that they must follow the school's instructions and guidance, and that he/she will report any questionable material they encounter to the teacher immediately.

Signed _____ Parent / Guardian

Date _____

When using computers, the Internet and electronic mail, I promise to follow the instructions and guidance given by my parents, teachers and other adults at the school.

Child's signature _____

Date _____

HESWALL PRIMARY SCHOOL

Dear Parents/Carers

Using Images of Children – Consent Form

As you know we take photographs of children in school. Some of these are used as evidence that children have undertaken a specific learning task, and these form part of your child's school record. We ask if we can use these images in our school's prospectus or in other printed publications that we produce, and we may ask if we can include them on our website. Occasionally children may be videoed for classroom use.

From time to time, our school may be visited by the media who will take photographs or film footage of a visiting dignitary or other high profile event, or a special event that is taking place in school, e.g. World Book Day. Pupils may appear in these images which may appear in local or national newspapers or on televised news programmes. Occasionally people who work with our children in school, e.g. Junior Chefs, wish to use photographs in their promotional materials.

Before we take a photograph, we need written consent in order to comply with the Data Protection Act 1998.

Please answer the following questions, then sign and date the form.

If the form is not signed, we cannot, and will not, use the photograph. We will not use the image(s) for any other purpose.

Yours sincerely
Jon Lawrenson
Headteacher

Name of Child: _____

Name of Parent/Guardian: _____

1. I understand and accept that my child's image will be used for use in school as evidence of your child's progress?	Yes / No
2. *I give permission for my child's image to be used in school, on our website and Twitter/Facebook feed?	Yes/No
3. I give permission for my child's image to be used in the school prospectus and other printed publications that we produce for promotional purposes?	Yes / No
4. Give permission for my child's image to be used in other printed publications for promotional purposes, e.g. local magazines, local businesses?	Yes / No
5. I understand that my child's name will only be used when recording evidence of my child's progress.	Yes / No

*Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

Signature of authorising adult: _____

Name of authorising adult (block capitals please) _____

Date: _____

HESWALL PRIMARY SCHOOL

USE OF INTERNET AND ELECTRONIC MAIL

CODE OF PRACTICE - STAFF

This document outlines the policy adopted by Heswall Primary School for the acceptable use of computer network facilities, including electronic mail and the Internet.

Anyone authorised to use such facilities is required to abide by the conditions laid down in this policy. Any breach of these conditions could result in disciplinary action or in some cases a criminal prosecution.

All users are expected to demonstrate a responsible approach to the use of resources available to them, and to show consideration for other users, both those using the school's facilities and those with whom they may come into contact on the Internet. Users are expected to behave in a legal, moral and ethical fashion that is consistent with school policies and standards.

It must be recognised that any view communicated over the Internet will be deemed to be the view of the school, and will in most cases be treated as equivalent to correspondence sent by traditional formal routes. Normal rules for authorising correspondence and statements should therefore be applied to electronic communication.

Access to the Internet by personal computers (including portables) provided by the school must use only the approved service providers. (Downloading 'free' browsers etc. may significantly change the way in which the PC is organised, which may in turn give rise to support problems.)

Users should print only essential material, and should check the length of a document before printing.

Use of the facilities provided will be routinely monitored and any unauthorised or unacceptable use could result in disciplinary measures.

Unacceptable Deliberate Use

The following activities, whilst not an exhaustive list, are unacceptable:

1. The access to, or creation, transmission or publication of, any offensive, discriminatory, pornographic, obscene or indecent images, sounds, data or other material.

2. The access to or creation, transmission or publication of, any data capable of being displayed or converted to such offensive, pornographic, obscene or indecent images, sounds, data or other material.

3. The creation, transmission or publication of any material which is designed or likely to cause offence, inconvenience or needless anxiety, or which may intimidate or create an atmosphere of harassment.

4. The creation, transmission or publication of defamatory material.

5. The receipt of transmission of material that infringes the copyright of another person.

6. The creation, transmission or publication of any material in violation of Data Protection legislation or of any UK or International laws or regulations. Such activity may constitute a criminal offence.

7. The transmission of unsolicited commercial or advertising material to other users of the Council's network or users of the internet.

8. The deliberate unauthorised access to facilities, services, data or resources which the school or any other network or service accessible via the Internet, or attempts to gain such access.

9. Unauthorised access to the electronic mail of another individual.

10. Deliberate activities with any of the following characteristics or that by their nature could result in:

    - Wasting staff or other users' efforts or network resources;
    - Corrupting or destroying other users' data;
    - Violating the privacy of other users;
    - Disrupting the work of other users;
    - Using the Internet in a way that denies service to other users (for example, by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading large files);
    - Continuing to use any item of software or to access any material after being requested to cease its use because of disruption caused to the functioning of the school's network or the Internet (for example utilities designed to broadcast network-wide messages);
    - The introduction or propagation of viruses.

11. Where the Internet is being used to access another network, any abuse of the acceptable use policy of that network.

12. Any use of the Internet or other facilities that could damage the reputation of the school.

USE OF INTERNET AND ELECTRONIC MAIL

Name: _____

I have read the Code of Practice and agree to abide by its terms and conditions.

Signed: _____

Date: _____