

# Hindley J and I School



## E-Safety Policy

**Written: March 2019**

**Awaiting Approval:**

**Signed by the Headteacher      date**

**Signed on behalf of the staff      date**

## **Introduction**

Resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. The use of digital technology and the Internet, by its nature, will however provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher.

The school has a duty to provide pupils with high-quality Internet access as part of their learning experience and therefore need to provide quality E-safety guidance to allow pupils to stay safe.

## **Aims**

The purpose of this policy is to:

- Establish the rules we have in school for using the internet and digital equipment/communications.
- Demonstrate the methods used to protect the children from sites containing inappropriate material.
- Demonstrate the methods used to keep the children safe.

The school believes that pupils accessing digital technology and the internet is an essential resource for supporting teaching and learning. The internet, and other digital technologies, open up opportunities for pupils and play an important role in their everyday lives.

We believe the benefits of using the internet, and other digital technologies far exceeds the disadvantages.

E-safety looks at the use of Internet technologies and electronic communications such as computers, tablets, games consoles and mobile phones. It looks at the personal publishing on social media. It highlights the need to educate children about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

- The Computing leader and Headteacher have been appointed the E-Safety leads.
- Our E-Safety Policy has been written and approved by staff and Governors.

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 Wigan LEA including the effective management of content filtering.

# The Internet

## 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 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. Our school has a duty to provide pupils with quality Internet access as part of their learning experience.

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;
- 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 Local Authority and DfE;
- Access to learning wherever and whenever convenient;
- Gaining an understanding of people and cultures around the world;
- Communicating with others in or out of the UK via online programs e.g. e-mails, blogging etc.

## World Wide Web

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.

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 be 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 educated in the actions to be taken when something inappropriate and upsetting is viewed.

## **Pupils' Access to the Internet**

- In school children will only normally use the Internet under supervision of an adult.
- The Computing Leader will have access to pupil's e-mails and other related files.
- Every child is allocated their own computer in the suite so that any violations can be linked to the child responsible.
- A Digital Device Allocation register will be complete by staff or pupils regarding the pupil allocation of tablets, laptops and computers in classroom sessions.
- Pupils and staff will be made aware and educated in the safe use of the internet and digital equipment/communications.
- Clear boundaries will be set and discussed with staff and pupils, for the appropriate use of the internet and digital communications.
- Pupils and staff will be made aware of the Securus monitoring system that checks that no illegal or inappropriate content is being accessed by users of computers in school.
- The Computing Leader will use Securus monitoring system to check that expectations of behaviour are being met by all users of computers in school.

## **Expectations of Pupils Using the Internet**

- All pupils must accept the terms of use before using the computers.
- At Hindley J & I School we expect all our pupils to be responsible for their own behaviour on the Internet. This includes materials they choose to access and the language they use.
- Pupils using the Internet are expected not to deliberately seek out offensive materials. Securus will alert the Computing Leader of any unsuitable content has been used and the child responsible will be made aware of their actions.
- Pupils are expected not to use any offensive language whilst using the internet e.g. in their e-mails, and will only contact people from our school or contacts the teacher has approved.
- Pupils must ask permission to use the Internet.
- No programs may be downloaded from the Internet.
- No personal details should be given out and no arrangements to meet someone should be made.
- Pupils choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.

## **School Website and Social Media Pages**

The school website and social media pages can celebrate good work, be used to contact parents, promote the school, publish resources and show links to other sites of interest.

We will only use the photographs of children when we have their parents' permission to do so.

Any photographs displayed on the website/media pages are property of the school and must not be used by anyone outside school.

# E-Safety

## Information System Security

- The school's ICT system security will be reviewed regularly. A virus protection will be installed and updated regularly.
- All staff laptops and data sensitive memory sticks will be encrypted.
- All staff iPads must be password protected.

## E-Mail

- Pupils and staff may only use approved e-mail accounts on the school systems.
- Pupils must be aware of how they can report abuse and who they should report abuse to.
- Pupils must immediately report to a staff member any incidence of offensive e-mails.
- Pupils must act responsible when sending e-mails and must not send any unpleasant, offensive material.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.
- Whole class or group e-mail addresses should be used in school.
- Access in school to pupils external personal e-mail accounts will be blocked.
- E-mail sent by pupils to external organisations should be written carefully and authorised before sending.

## Social Networking

- Access to social networking sites and newsgroups will be blocked / filtered unless a specific use is approved.
- E-Safety lessons are arranged termly to educate pupils on the safe use and dangers of social media sites and chat rooms.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must be aware of how they can report abuse and who they should report abuse to.
- Pupils should be advised about the reasons why personal photos should never be posted on any social network space without considering how the photograph could be used now or in the future.
- Pupils should be taught about the responsibility of using social networks and about inappropriate behaviour e.g. send any unpleasant, offensive material.
- Pupils should be advised on security and encouraged to use nicknames, set strong passwords, to deny access to unknown individuals and how to block unwanted communications
- Pupils should only invite known friends and deny access to others.

## **Filtering**

- The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.
- A filtered Internet Service is in place that minimises the chances of pupils encountering undesirable material.
- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager. This information will also be available through school's Securix e-safety system.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Website can be released from the filter but only with permission from the head.
- Any websites deemed unsuitable will be placed under the filtering service.

## **Videoconferencing & Social Media Video Calling**

- Videoconferencing/video calling should use the educational broadband network or a trustworthy provider to ensure security and quality of service.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing/video calling will be appropriately supervised and be suitable for the pupils' age.
- The school will educate the children in the safe use of social media video use.

## **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.
- Pupil should be taught the dangers of new social networking Apps.

## **Protecting Personal Data**

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

## **Published content - the school website and social media pages**

- 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 Computing Leader and staff will take editorial responsibility and ensure that content is accurate and appropriate.

## **Publishing pupil's images and work**

- Photographs that include pupils will be selected carefully so that images of individual pupils cannot be misused.
- Pupils' full names will not be used anywhere on the website or other social media pages, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media pages.
- Any photographs displayed on the website/social media pages are property of Hindley J & I and must not be used by anyone outside school.

## **Mobile Phones**

### **Appropriate use of Mobile Phones in School**

At Hindley Junior and Infant School, the welfare and well-being of our pupils is paramount and we are committed to ensuring the safety of children in our care. We recognise the importance of mobile phones in school for communication purposes, but are aware that casual or inappropriate use of mobile phones in the School could pose a risk to children.

### **Pupils**

At Hindley Junior and Infant school we understand that some pupils are given permission to travel to and from school independently. For their safety they may bring their named mobile phone into school however it should be switched off and placed in the basket in the classroom. Any inappropriate use of mobile phones will not be tolerated and the pupil will no longer be given permission to bring their device to school. Hindley Junior and Infant School are not responsible for any loss or damage to any mobile phones.

### **Staff**

Staff members are not allowed to use their mobile phones in the classroom whilst children are present. The use of their phone to take photographs or videos of children is strictly prohibited. All staff members should provide their next of kin with the school office number to contact in the event of an emergency.

### **Visitors**

The school will display a notice advising visitors that mobile phones are to be handed in at the School Office. The mobile phone should be switched off and will be placed in the school safe. If this is not possible, then mobile phones should be switched off and kept out of sight.

### **Parents and Carers**

During events in school e.g. Christmas performances, class assemblies etc. A member of the Senior Leadership Team will inform parents to switch all mobile phones off to ensure there are no interruptions. Videoing is strictly prohibited. Parents may take photographs ***after the performance*** of their own child/children in costume at the discretion of the Senior Leadership Team.

## **Assessing Risks**

- 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. Neither the school nor Wigan Council can accept liability for the material accessed, or any consequences of internet access.
- The school will 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 reported to the E- safety Leader and action taken with Wigan's Safeguarding Children Board e-Safety policy will be taken.
- Any staff misuse that suggests, a child has been harmed or that a member of staff is unsuitable to work with children must be dealt with in accordance with school child protection procedures.
- Any complaint about staff misuse must be referred to the Headteacher and if the misuse is by the Headteacher it must be referred to the Chair of Governors in line with the Wigan Safeguarding Board Child Protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

# **Communication of the E-Safety Policy**

## **Pupils**

### **Pupils are informed of the elements of e-safety.**

- Pupils are informed of the filtered Internet Service in place that minimises the chances of pupils encountering undesirable material.
- Pupils are informed about the security software used that monitors the network and internet use.
- Age appropriate e-safety lesson will be delivered on a regular basis along with PHSE lessons/assemblies.
- Posters reminding pupils of Internet safety and Cyberbullying will be displayed around school.

## **Staff**

- All staff will be given the Schools 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.

## **Parents**

- Parents' and carers' attention will be drawn to the school E-Safety policy in newsletters, the school brochure and on the school website.
- Parents and carers will from time to time be provided with additional information on e-safety.

At the beginning of each academic year parents will be asked to read and sign the school's Parent Consent Form. On doing this they must indicate that they agree to our Pupil Internet Agreement and they may indicate that they agree to our Photographs in School Consent.

## **PUPIL INTERNET AGREEMENT**

At Hindley J and I we expect all pupils to be responsible for their own behaviour on the internet. This includes the materials they choose to access and the language they use. Pupils must ask permission before accessing the Internet.

Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupil encounter such material accidentally, they are expected to turn the screen off and report it immediately to a member of staff.

Pupils are expected not to use any inappropriate language in their e-mail communications and contact only people they know or those who a teacher or teaching assistant has approved. No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project. It is forbidden to be involved in the sending of chain letters.

Pupils should not access other people's files unless permission has been given. Computers should only be used for schoolwork and homework unless permission has been granted otherwise.

No program files may be downloaded to the computer from the Internet. No programs on disc or CD Rom should be brought in from home for use in school. Personal printing is not allowed on our network for cost reasons unless permission has been granted from the teacher.

Pupils consistently choosing not to comply with these expectations will be warned and subsequently may be denied access to internet resources.

# PHOTOGRAPHS IN SCHOOL CONSENT FORM

The school may hold photographs or images in either paper or electronic form. We also use photographs and video images in the classroom and around the school.

Photographs and videos may be published on Class Dojo which is only available to the staff and parents of Hindley J and I School.

Photographs and or videos are also used on the Hindley J and I School Website and on our official social media pages which can be accessed by the general public.

In addition we use the local press to celebrate achievement and they take individual and group photographs which are published by them.

Please note- If your child takes part in an activity run by an outside provider, it is your responsibility to carefully check any agreement you sign with them. Allowing photographs and videos to be used for educational purposes is sometimes part of their contract.

*See below an example of our consent form:*

## Hindley Junior and Infant School

### Annual Parental Consent Form

Child's Name \_\_\_\_\_

Class \_\_\_\_\_ Academic Year \_\_\_\_\_

After reading all the information enclosed this front page is to be completed by the Parent/Carer to give permission for the following:

Use of Internet within school

Photograph Permission

Tick all the boxes giving your consent on behalf of your child.

# Staff Information Systems Code of Conduct

**To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's E-Safety policy for further information and clarification.**

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school E-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

**I have read, understood and agree with the Information Systems Code of Conduct.**

Signed: ..... Capitals: ..... Date: .....

Accepted for school: ..... Capitals: .....