Hindley Sure Start Nursery
E-Safety Policy

Our e-Safety Policy has been written by the school, building on government guidance. It has been agreed by the Senior Leadership Team and approved by governors.

Why is Internet use important?

The internet is an essential element in 21st century life for education, business and social interaction. Internet use is a key learning tool for all pupils, staff, visitors and members of the community. The Internet may be widely used outside of the school and centre and pupils and visitors 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;
- Vocational, social and leisure use in libraries, clubs and at home;
- 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;

Access to learning, wherever and whenever convenient.

How can Internet use enhance learning?

- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils, staff and visitors learn how to evaluate Internet content?

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught of the materials they need.

.

How will information systems security be maintained?

- The server operating system will be secured and kept up to date.
- Virus protection for the whole network will be installed and current.

Access by wireless devices will be pro-actively managed. Wide Area Network (WAN) security issues include:

- The security of the school information systems is reviewed regularly by the local authority;.
- Virus protection will be updated regularly;
- Unapproved system utilities and executable files will not be allowed in work areas or attached to an e-mail;
- Files held on the school's network will be regularly checked;

How will email be managed?

- Pupils will not have the facility to access any e-mail accounts.
- The pupil and centre pc's will not have the facility to access any email accounts.
- Access in the school and centre 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.

How will published content and the school website be managed?

- The contact details on the school website should be the school address, e-mail and telephone number.
- Staff or pupils' personal information must not be published.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- The Headteacher will take overall editorial responsibility and ensure that the content is accurate and appropriate.

Can pupils' images or work be published?

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.
- Work can only be published with the permission of the pupil and parents.
- Parents are clearly informed of the school and centre policy on image taking and publishing.

How will social networking and personal publishing be managed?

- The local authority and school will block/filter access to social networking sites. Newsgroups will be blocked unless a specific use is approved.
- Pupils, staff and visitors will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, instant Messaging and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupil, staff and visitors should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas.
- Advice should be given regarding background detail in a photograph which could identify the student/visitor or his/her location e.g. house number, street name or school.
- Students should be advised not to publish specific and detailed private thoughts. Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

How will filtering be managed?

- The school will work with the LA and RM Filtering Services to ensure that systems to protect pupils, staff and visitors are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to the Business Manager. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The local authority uses filtering software on its servers. A key feature of the filtering software is the ability to categorise websites and then allow or restrict users' access by selecting categories.
  .

How will videoconferencing be managed?

Videoconferencing is not used at Hindley Sure Start, due to the age range of our pupils. However, if it was to be used, the following would be adhered to and put into practice:

- The equipment and network Internet Protocol videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name. External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school Website. Users Videoconferencing should be supervised appropriately for the pupils' age Content.
- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely. If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights. Establish dialogue with other conference participants before taking part in a videoconference.

- If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school and centre is allowed.

Protecting Personal Data

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

How will Internet access be authorised?

- The school will authorise internet access to those staff who have children's centre server access, which is monitored through the local authority IT department.
- Staff working in class will be taught internet access through whiteboard interaction for the children.

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school and centre should audit ICT use to establish if the E-Safety Policy is adequate and that the implementation of E-Safety Policy is appropriate and effective.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

How will e-Safety complaints be handled?

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Staff, parents and stakeholders will be informed of the complaints procedure

Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the school E-Safety Policy in newsletters and on the school website

Some simple dos and don'ts regarding e-safety

Working online

Do

- Make sure that you follow Hindley Sure Start policies on keeping your computers up to date with the latest security updates.
- Make sure that you keep any computers that you own up to date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Get advice from your IT team if you need help.
- Only visit websites that are allowed by Wigan Council. Remember the local authority may monitor and record (log) the websites you visit.
- Turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer and attack and forgery site warnings in Mozilla Firefox.)
- Make sure that you only install software that the local authority has checked and approved
- Be wary of links to websites in emails, especially if the email is unsolicited
- Only download files or programs from sources you trust. If in doubt, talk to the Business Manager.
- Check that you follow the Hindley Sure Start Acceptable Use Policy

Email and messaging

Do

- Read Hindley Sure Start Email policy.
- Report any spam or phishing emails to the Business Manager that are not blocked or filtered

Don't

- Click on links in unsolicited emails. Be especially wary of emails. requesting or asking you to confirm any personal information, such as passwords, bank details and so on.
- Turn off any email security measures that the local authority or Hindley Sure Start has put in place or recommended.
- Email sensitive information unless you know it is encrypted. Talk to the Business Manager for advice.
- Try to bypass Wigan Council security measures to access your email off-site (for example, forwarding email to a personal account)
- Reply to chain emails.

Passwords

Do

- Follow Hindley Sure Start and Wigan Council password policy
- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers)
- Make your password easy to remember, but hard to guess
- Choose a password that is quick to type
- Use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password. Change your password(s) if you think someone may have found out what they are.

Don't

- Share your passwords with anyone else
- Write your passwords down
- Use your work passwords for your own personal online accounts
- Save passwords in web browsers if offered to do so
- Use your username as a password
- Use names as passwords
- Email your password or share it in an instant message.

Laptops

Do

- Shut down your laptop using the 'Shut Down' or 'Turn Off' option
- Try to prevent people from watching you enter passwords or view sensitive information
- Turn off and store your laptop securely (if travelling, use your hotel's safe)
- Use a physical laptop lock if available to prevent theft
- Lock your desktop when leaving your laptop unattended
- Make sure your laptop is protected with encryption software.

Don't

- Store remote access tokens with your laptop
- Leave your laptop unattended unless you trust the physical security in place
- Use public wireless hotspots – they are not secure
- Leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- Let unauthorised people use your laptop
- Use hibernate or standby.

Sending and sharing

Do

- Be aware of who you are allowed to share information with. Check with your Information Asset Owner if you are not sure. (Business Manager or local authority).
- Ask third parties how they will protect sensitive information once it has been passed to them
- Encrypt all removable media (USB pen drives, CDs, portable drives) taken outside your organisation or sent by post or courier.

Don't

- Send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives) if secure remote access is available
- Send sensitive information by email unless it is encrypted
- Place protective labels on outside envelopes. Use an inner envelope if necessary. This means that people can't see from the outside that the envelope contains sensitive information.
- Assume that third-party organisations know how your information should be protected.

Working on-site

Do

- Lock sensitive information away when left unattended
- Use a lock for your laptop to help prevent opportunistic theft.

Don't

- Let strangers or unauthorised people into staff areas
- Position screens where they can be read from outside the room.

Working off-site

Do

- Only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above.
- Wherever possible access data remotely instead of taking it off-site
- Be aware of your location and take appropriate action to reduce the risk of theft
- Make sure you sign out completely from any services you have used
- Try to reduce the risk of people looking at what you are working with

- Leave your laptop behind if you travel abroad (some countries restrict or prohibit encryption technologies).

This policy is to be read in conjunction with the following policies:

Email policy
Data Policy
Internet policy
IT Acceptable Use Policy
Laptop Policy
Hardware Policy
ICT Security Policy

Date _____ approved.

Signed _____ Headteacher

Signed _____ Chair of committee

Reviewed April 2014, April 2016