Internet Policy

Written By: H. Walker
Last Reviewed: October 2020
Adopted by Governors:
Next Review: October 2022

1. Introduction:

The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet.
- Demonstrate the methods used to protect the children from inappropriate sites.
- Outline pupil and staff responsibilities.
- Demonstrate parental involvement in the protection process.

The school believes that the benefits to pupils from access to the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians. This is why we ask both pupils and parents to sign a copy of the pupil Acceptable Use Policy, which is stored with the child's admission records.

At Highfields, we feel that the best recipe for success lies in a combination of site-filtering, supervision and by fostering a responsible attitude in our pupils in partnership with parents.

2. Using the Internet for Education:

The school intends to teach pupils about the vast information available on the Internet, using it as a planned part of many lessons. With the wireless network, access to the Internet can take place throughout the school at any time, ensuring web-based materials can be utilised to maximum efficiency.

All staff will review, evaluate and share resources available on web sites appropriate to the age range and ability of the pupils being taught. The Computing Subject Champion will assist in the dissemination of this information using the termly unit plans. If staff find any issues with the use of the internet, they need to report these to the ICT technician immediately – especially if the issues are regarding E-Safety.

Children may be given tasks to perform using a specific group of web sites. Sometimes, pupils may use a child-friendly search engine such as: www.askkids.com or Searchypants to find appropriate images or web-based information. Tasks will be set to encourage pupils to view web sites and information with a critical eye, challenging the authenticity and validity of non-trusted websites.

3. Pupils' Access to the Internet:

Highfields will use Trustnet's 'filtered' Internet Service, which will minimise the chances of pupils encountering undesirable material. If any materials are found by pupils or staff which are deemed inappropriate, these must be reported to the ICT technician as soon as possible so that the content can be made aware of and blocked.

Highfields will only allow children to use the Internet when there is a responsible adult present to supervise. However it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen, so there is an element of trust with all children when the internet is being used. If children are using the internet irresponsibly, then children may be asked to stop using the internet for a period of time (depending on the reason they have been asked to stop).

Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, the expectation we have of them. Web-based teaching materials will be built into ICT schemes and class assemblies to reinforce key online safety messages. Parents will be supported with web-safety updates; workshops when needed and links to useful websites. The Digital Leaders will continue to support E-Safety messages across school to spread the message to the rest of the children.

4. Expectations of Pupils Using the Internet:

- At Highfields, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access and language they use.
- Pupils using the internet are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider (Trustnet) or technician can block further access to the site.
- Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved (such as French pen pals).
- They are taught the rules of etiquette in email in Y3 (younger pupils are not granted access to emails) and are expected to follow them.
- Pupils must ask permission before accessing the Internet and have a clear idea why they are using it.
- Pupils should not access other people's files unless permission has been given by the class teacher.
- 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. This is to prevent corruption of data and avoid viruses.
- Homework completed at home may be brought in on disc or memory stick but the class teacher should obtain the data from this.
- 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.
- Web cameras may be used if part of a school project **under strict adult supervision** and only if the adult has checked the contact first.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources. They will also come under the general discipline procedures of the school alongside the school behavior policy.

Pupils will be asked to sign this agreement, ensuring that they are aware of expectations. Parents will also need to sign copies of this agreement and will be expected to shadow these rules for their children's safety at home. All children in school will have been given a copy of this from N – Y6. The Acceptable Use Policy is stored with the child's admission records.

5. Staff Responsibilities:

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of governors, aims to embed safe practices into the culture of the school. The Headteacher and E-safety Coordinator ensure that the policy is implemented and compliance with the policy monitored.

The responsibility for E-Safety has been designated to a member of teaching staff.

Our school **E-Safety Coordinator** is Miss H Walker

Our E-Safety Coordinator ensures they keep up to date with E-Safety issues and guidance through liaison with the Local Authority e-Safety Officer (Sue Courtney-Donovan) and through organisations such as BECTA and The Child Exploitation and Online Protection (CEOP). The school's E-Safety Coordinator ensures the Head, senior management and governors are updated as necessary when a problem arises or a policy is renewed.

All staff working with children are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures:

Working Online:

- Make sure that you only install software that the ICT technician has checked and approved.
- Report any spam or phishing emails to the ICT technician that are not blocked or filtered.
- Email school-related information using your 365 address and not personal accounts such as Googlemail Or Hotmail.
- No member of staff should download apps or make modifications to iPads apart from the Computing Subject Champion

Passwords:

- 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.
- **Don't share your passwords with anyone else.**
- Don't write your passwords down.
- Don't email your password or share it in via a message.

Laptops:

- At the end of the day, shut down your laptop using the 'Shut Down' or 'Turn Off' option, don't leave it switched on.
- Try to prevent people from watching you enter passwords or view sensitive information.
- Don't leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- Don't let unauthorised people use your laptop. Your laptop is for use at school.
- Don't store sensitive data on your laptop. All sensitive data should be stored on encrypted memory sticks.
- No information should be stored on the desktop of the laptop.

Memory Sticks:

- Resources can be stored on non-encrypted memory sticks providing they do not contain any information about the children or school.
- Ensure **ALL** sensitive school data (such as IPPs, data, medical records) are stored on the encrypted memory stick provided by the school.

Working On-site:

- Don't let strangers or unauthorised people into the staff ICT area (Staff Share).
- Don't position screens where they can be read from outside the room (especially in offices).
- Make sure computers are locked or logged off at night. **Computers should not be left logged on at night, this could be a data protection breach.**

Working Off-site:

- Only take offsite information you are authorised to and only when it is necessary.
- Access pupil data via Office 365, which is a secure platform.

- Encrypted memory sticks should be used with school's laptops and safe computer systems. They should not be used on any **public** computer system or network.

Personal Data:

- IPPs, assessment records, pupil medical information and any other data related to pupils or staff **should not** be stored on personal memory sticks but stored on encrypted USB memory sticks provided by school or on our secure Office 365 learning platform or Staff Share drive.

Social Networking Sites:

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position.
- Under no circumstances should present or past school pupils be added as friends.
- Staff should be mindful about what they put on social media sites (both photos and posts) ensuring that they maintain a level of professionalism at all times (especially if they are friends with friends of parents).
- Make sure that any profiles are kept private to eliminate the chances of information being leaked.
- Under no circumstances should any reference to pupil's name or work be made on any social network site.
- Under no circumstance should any images of school children be used on social networks, including images in the background of other images.
- Any photographs taken inside school should not make the school identifiable and should certainly **not** show any pupils.

Members of staff who breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

6. Complaints Procedure:

As with other areas of school, if a member of staff, a child or a parent/carer has a complaint relating to E-Safety, then they will be considered and prompt action will be taken. Complaints should be addressed to the E-safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the leadership team and those members directly involved.

7. Updating the Policy:

This policy will be updated again in October 2022.

Data Security

Highfields Primary School

Following a review of procedures in place to store sensitive data in line with National recommendations the following practice is to be adhered to:-

Sensitive data consists of any information which is personal to individuals or deemed sensitive or valuable to the school.

Staff should only save sensitive data in the following secure formats: -

1. On the learning platform (Office 365)
2. On the Staff Share drive
3. On the encrypted USB memory stick provided. The only USB sticks that should be used to store any sensitive data are those provided, which are already encrypted, by the school.

This ensures that no legal action can be taken for lost data.

If you lose your encrypted memory stick or are unable to open it because of a password error, you must inform the ICT technician without delay. It is imperative that you do not share or write down your password. You may add a question prompt reminder when first accessing your memory stick, which can be used if you have forgotten your password. It is your responsibility to keep the data from your memory stick regularly backed up in another secure format, the best way to do this would be to use the Office 365 learning platform.

Failure to follow these guidelines will be treated seriously and could lead to disciplinary procedure.

H. Walker
October 2020

I understand the procedures and agree to follow them with immediate effect

Name _____

Signed_____