NORTHMEAD JUNIOR SCHOOL

Internet Safety Policy

Overview

This Internet Safety policy was created to safeguard the pupils at Northmead Junior School from any form of inappropriate use of technology. It sits alongside all e-safety policies already in place. As a school, we recognise that technology plays an important and positive role in children's lives, both educationally and socially. We are committed to helping all members of our school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly.

The following Policy is based on Department for Education guidance, in collaboration with EXANetworks.

Introduction School Aims

Our Internet Safety policy reflects our school aims which are:

- To provide a broad and balanced curriculum that ensures each child has a high quality, stimulating, varied and inclusive learning experience, which encourages creativity, enjoyment and excellence.
- To build committed, supportive and effective teams, operating within a united whole.
- To develop self-esteem and a positive attitude towards others.
- To raise each child's expectation of what they can achieve both now and in preparation for adult life

Policy Aims

The aims of this policy are to ensure that:

- Pupils, staff and parents are educated to understand the need to use the Internet safely and appropriately and what the consequences of careless or inappropriate use can be
- Knowledge, policies and procedures are in place to ensure all staff and pupils are given the skills to empower them and prevent incidents of inappropriate use in school or within the school community
- There are measures in place to deal effectively with cases of inappropriate use
- The Leadership team monitor the effectiveness of implementation of procedures to encourage positive use/behaviour.

Technical and Infrastructure approaches

This school:

- Has an educational filtered secure broadband connectivity through EXANetworks and so connects to the 'private' National Education Network;
- Uses the EXANnetworks filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the pupils;
- Ensures network health through use of reputable anti-virus software etc and network set-up so staff and pupils cannot download executable files;
- Uses individual, audited log-ins for all users;
- Uses Department for Education (DfE), Local Authority (LA) or EXANetworks approved systems to store personal data
- Blocks all Chat rooms and social networking sites except those that are part of an educational network;
- Only unblocks other external social networking sites for specific educational reasons;
- Provides all staff with secure remote access to the school server;
- Uses security time-outs on Internet access where practicable / useful;
- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Works in partnership with the EXANetworks to ensure any concerns about the system are communicated so that systems remain robust and protect pupils;
- Ensures the Systems Administrator / network manager is up-to-date with EXANetworks services and policies / requires the Technical Support Provider to be up-to-date with EXANetworks services and policies;

Policy and procedures

This school:

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and pupils have signed an acceptable use agreement form and understand that they must report any concerns. Copies to be kept on file. Explained to pupils and used as part of the teaching programme.
- Requires staff to preview websites before use.
- Requires staff to plan the curriculum context for Internet use to match pupils' ability, using child friendly search engines where more open Internet searching is required; eg Youtube for kids
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs users that Internet use is monitored;

- Informs staff and pupils that that they must report any failure of the filtering systems directly to the IT Technician;
- Requires parents/carers to countersign pupil acceptable use agreement forms;
- Ensures parents provide consent for pupils to use the Internet, as well as other IT technologies, as part of the acceptable use agreement form at time of their child's entry to the school;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record of any online bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Provides e-safety advice for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and training:

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report any abuse;
- Has a clear, progressive e-safety education. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - SMART – using SMART rules to stay safe online, to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour;
    - keeping personal information private;

  - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - to understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;
  - to understand why they should not post or share detailed accounts of their personal lives, contact information (personal information including full name, email address, phone number, address etc unless parents or teachers are aware), daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - to understand why they must not post pictures or videos of others without their permission;
  - to know not to download any files – such as music files - without permission;
  - to have strategies for dealing with receipt of inappropriate materials;

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line;
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to handle such data within the school system;
- Makes training available annually to staff on the e-safety education program;
- Runs a rolling programme of advice, guidance and training for parents, including:
  - Information leaflets;
  - in school newsletters;
  - on the school web site;
  - distribution of National Onine Safety resources for parents materials
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

Appendix 1 Internet policy and procedures: background information

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. **Supervision is the key strategy.** Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation.

Surfing the Web

It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question “Why are we using the Internet?”

Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. It is not sensible to have younger pupils ‘searching the Internet’.

Pupils do not need a thousand Web sites on weather. A small selection will be quite enough choice, and as with other resources, the teacher needs to have checked and selected them so they are appropriate for the age group and fit for purpose. Favourites / bookmarks are a useful way to present this choice to pupils.

Teachers' web site selections for various topics can be put onto a topic page in the Classroom area of the server for easy pupil access.

Hackers can infiltrate a site or take over the domain, resulting in a previously acceptable site suddenly changing. Therefore, sites should always be previewed and checked.

Search Engines

Some common Internet search options are high risk, for example 'Google' image search. Some LAs and Councils block this. Others keep it unblocked because it can be a useful tool for teachers looking for images to incorporate in teaching. Where used – it must be with extreme caution. Google image search can be set-up to run in 'safe' mode although this is not fully without risk.

Images usually have copyright attached to them which is an issue commonly overlooked but a key teaching point to pupils and staff.

Collaborative Technologies

There are a number of Internet technologies that make interactive collaborative environments available. Often the term 'social media' is used. Examples include blogs (personal web-based diary or journals), wikis (modifiable collaborative web pages), and podcast sites (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web). Using these technologies for activities can be motivational, develop accuracy and presentations skills, helping children consider their content and audience. Be aware of the dangers around using the internet and only use trusted sites.

Webcams and Video Conferencing

Webcams: are used to provide a 'window onto the world' to 'see' what it is like somewhere else. Pupils can search on the Internet for other webcams - useful in subject study such as geography (e.g. to observe the weather or the landscape in other places). However, there are risks as some webcam sites may contain, or have links to adult material. In schools, adult sites would normally be blocked but teachers need to preview any webcam site to make sure it is what they expect before ever using with pupils.

The highest risks lie with streaming webcams [one-to-one chat / video] that pupils use or access outside of the school environment. Pupils need to be aware of the dangers. Pupils will never be asked to access any service that allows face-to-face chatroom style video calling whilst in school.

Social Networking Sites

These are a popular aspect of the web for young people. Sites such as Facebook, Instagram, YouTube, snapchat, Twitter, Tumblr, TikTok, Kik, and Whatsapp allow users to share and post web sites, videos, podcasts etc. It is important for children to understand that these sites are public spaces for both children and adults. They are environments that should be used with caution. Users, both pupils and staff, need to know how to keep their personal information private and set-up and use these environments safely. [See E-safety programme]

Most schools will block such sites. However, pupils need to be taught safe behaviour as they may well be able to readily access them outside of school. Parents and children are reminded that a lot of these websites enforce age restrictions to own an account.

Podcasts

Podcasts are essentially audio files published online, often in the form of a radio show but can also contain video. Users can subscribe to have regular podcasts sent to them and simple software now enables children to create their own radio broadcast and post this onto the web. Children should be aware of the potentially inappropriate scope of audience that a publicly available podcast has.

Chatrooms

Many sites allow for 'real-time' online chat. Again, children should only be given access to educational, moderated chat rooms. The moderator (or referee) checks what users are saying and ensures that the rules of the chat room (no bad language, propositions, or other inappropriate behaviour) are observed. Pupils should be taught to understand the importance of safety within any chat room because they are most likely at risk out of school.

Sanctions and infringements

The school's Internet e-safety / Acceptable Use policy is available and explained to staff / Governors, pupils and parents, with all signing acceptance / agreement forms appropriate to their age and role. The school has clear possible sanctions for infringements.

Following any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on school computers, the matter will be immediately referred to the Police.

Date of review	Autumn 2020
Date of next review	Autumn 2021