PINEWOOD INFANT SCHOOL AND FOUNDATION UNIT

E SAFETY POLICY

Autumn 2017

Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to arm our young people with the skills to access lifelong learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies which children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Pinewood Infant School we understand the responsibility to educate our pupils on internet safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

'Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach… Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks'

BECTA Safeguarding Children Online Feb 2009

This internet safety policy will reflect the need to raise awareness of the safety issues associated with information systems and electronic communication as a whole.

Whole School Approach to the safe use of ICT

- The internet is an essential element for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
- An effective range of technological tools
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils
- Policies and procedures, with clear roles and responsibilities

Internet use will enhance learning

The school internet access is designed for pupil use and includes filtering appropriate to the ages of pupils.

- Pupils will be taught what internet use is acceptable and what is not and 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.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

Roles and Responsibilities

Internet is recognised as an essential aspect of strategic leadership in this school and the head teacher, with the support of the Governors, aims to embed safe practises into the culture of the school. The head teacher ensures that the policy is implemented and has ultimate responsibility to ensure that the policy and practises are embedded and monitored.

The named internet safety co-ordinator in our school is Kellie Reilly

It is the role of the internet safety co-ordinator to keep abreast of current issues and guidance through organisations such as Notts LA, CEOP (Child Exploitation and Online Protection) and Child Net.com.

The internet safety co-ordinator ensures the head teacher; senior management and governors are updated as necessary.

All teachers are responsible for promoting and supporting safe behaviour in their classroom and following school internet safety procedures.

All staff should be familiar with the school's policy including;

- safe use of e-mail (via Office 365)
- safe use of the internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website
- their role in providing internet safety education for pupils
- staff are reminded/updated about internet safety regularly and new staff receive information on the school's acceptable use policy as part of their induction
- staff are reminded that their access to the school portal (remote access) should be secure

Managing the school internet safety messages

- We endeavour to embed internet safety messages across the curriculum whenever the internet and/or related technologies are used.
- The internet safety policy will be shared with new staff, including the acceptable use policy as part of their induction.
- Internet safety posters including the SMART rules will be prominently displayed in each classroom.
- An annual internet safety day is held every year.
- All children and parents/carers are required annually to sign our 'Acceptable Use of Computing and Internet agreement'

Internet safety in the curriculum

- ICT and online resources are increasingly used across the curriculum. We believe it is essential for safety guidance to be given to the pupils on a regular and meaningful basis.
- We continually look for new opportunities to promote internet safety.
- We provide opportunities within a range of curriculum areas to teach about internet safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling, and activities as part of the Computing curriculum.
- Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies

Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- Pupils will have supervised access to internet resources through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents/carers re-check these sites and supervise this work. Parents/carers will be advised to supervise any further research.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the internet safety co-ordinator where the incident will be recorded in the e-safety log book.
- It is the responsibility of the school, by delegation to Notts CC Service desk, to ensure that antivirus protection is installed and kept up-to-date on all school machines.
- Staff have access to Microsoft Office365. All their accounts can be accessed/managed by the computing coordinator

E-mail

The use of email within school is an essential means of communication for staff.

- The school gives staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact pupils using personal email addresses.
- Staff must inform the internet safety co-ordinator if they receive an offensive e-mail.

Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- in display material that may be used in the school's communal areas
- on the digital screen situated in the school playground

Children's names will not be published alongside their image and vice versa without permission from the parents. E-mail and postal addresses of children will not be published. Children's full names will not be published.
Before posting children's work on the internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Social networking and personal publishing

Caution is used when accessing social networking sites at home by all staff and they are not allowed to include parents of the school in their social contact unless they are a family member or friend separate to school. As part of the internet safety education programme children and parents will be advised that social networking sites are not appropriate for Infant aged children, children will be taught about the potential risks and how to keep personal information safe.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training on acceptable use, social media risks, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- No reference is made in social media to pupils, parents/guardians or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk or loss of personal information.

Notts CC blocks/filters access for pupils to social networking sites.

Video Conferencing

- Permission is sought from parents and guardians if their children are involved in video conferences
- All children are supervised by a member of staff when video conferencing

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

- Mobile phones will not be used in school for personal use except in named zones.
- Mobile phones will be kept away from children at all times.
- The sending of abusive or inappropriate text messages is forbidden.
- Ipads & their apps will be closely monitored – a username/password is required for downloading new apps.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The children are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and children are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Key stage 1 and foundation pupils use a generic user name to access the school network.
- Children are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others.
- If a password may have been compromised or someone else has become aware of the password the child or adult must report this to the internet safety co-ordinator
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically.
- Individual staff users must also make sure that workstations are not left unattended and are locked. This includes remote access.

- A copy of staff email passwords and children's individual passwords will be kept in a safe and secure area by the computing coordinator.

Data protection

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

- Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school/children/pupil data.

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Cyberbullying

The increasing use of digital technology and the internet has also provided new and particularly intrusive ways for bullies to reach their victims. Cyberbullying can take many forms and bullying online can often start in school and then be progressed online or start online and influence behaviour in school.
Whilst most incidents of Cyberbullying occur outside school we will offer support and guidance to parents/guardians and their children who experience online bullying and will treat Cyberbullying with the same severity as any other forms of bullying.
Cyberbullying can include:

- hacking into someone's accounts/sites
- posting prejudice/hate messages
- impersonating someone on line
- public posting of images
- exclusion
- threats and manipulation
- stalking

We will ensure that our children are taught safe ways to use the internet and encourage good online behaviour.

Bullying can take place between:

- young people
- young people and staff
- between staff
- individuals or groups

Responding to internet safety incidents/complaints

As a school we will take all reasonable precautions to ensure internet safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor Nottinghamshire LA can accept liability for material accessed, or any consequences of internet access. Complaints relating to internet safety should be made to the internet safety co-ordinator. Any complaint about staff misuse must be referred to the Head teacher. Incidents will be logged.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the internet safety co-ordinator.

• Deliberate access to inappropriate materials by any user will lead to the incident being logged by the internet safety co-ordinator, depending on the seriousness of the offence; investigation by the head teacher/Notts LA may lead to immediate suspension, possibly leading to dismissal and involvement of the police for very serious offences.
• Children and parents/carers will be informed of the complaints procedure.
• Parents/carers and children will need to work in partnership with staff to resolve issues.

Radicalisation and the use of social media to encourage extremism

The internet and in particular the use of social media has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as extreme ideological views. The use of social media and the internet as tools to radicalise young people cannot be underestimated. We recognise that those that seek to recruit young people to follow extremist ideology often target those who are already vulnerable in some way and that exposure to extreme views can make young people vulnerable to further manipulation and exploitation. This has led to social media becoming a platform for:

- intensifying and accelerating the radicalisation of young people
- confirming extreme beliefs
- access to like-minded people and creating an online community
- normalising abnormal views and behaviours

We have a number of measures in place to help prevent the use of social media for this purpose:

- website filtering is in place to help prevent access to Daesh, AQ, Far Right, Neo Nazi, White Supremacist ideology, Irish Nationalist and Loyalist paramilitary groups, and extremist Animal Rights movements.
- website filtering blocks access to social media sites such as Facebook, Snapchat, Instagram and Twitter
- pupils, staff and parents are educated in safe use of social media, privacy settings, parental controls and the risks posed by online activity, including that from extremist and far right groups.

Dealing with possible incidents

All staff receive training, advice and support on protecting children from the risk of online radicalisation. We ensure staff have the knowledge and confidence to identify children at risk. Staff safeguard and promote the welfare of children and know where and how to report possible incidents. In the event of prejudicial behaviour staff must;

- report the incident to the Senior Designated Safeguarding Lead, Rachel Otter
- or in the absence of the Senior Designated Safeguarding Lead, the deputy Senior Designated Lead, Claire Reville or member of the Senior Leadership Team
- all incidents will be fully investigated and recorded in line with our Safeguarding and Behaviour policies and records will be kept in line with procedures for any safeguarding incident
- The TECT team should be contacted in the first instance for advice and support. If the concern is more serious then we would contact the police prevent team prevent@nottinghamshire.pnn.police.uk and refer to the channel panel if required.
- If it is deemed necessary parent/carers will be contacted and the incident discussed in detail, aiming to identify motivating factors, changes in circumstances at home, parental views of the incident and to assess whether the incident is serious enough to warrant a further referral
- The incident will be recorded in the e-safety log

Equal Opportunities

Pupils with additional needs:
Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of internet safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of internet safety. Internet activities are planned and well managed for these children.

Reviewing this Policy

There will be an on-going opportunity for staff to discuss with the internet safety co-ordinator any issue of safety that concerns them.

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or the Government change the orders or guidance in any way.