NEWBRIDGE
PREPARATORY SCHOOL

E-SAFETY POLICY

INTRODUCTION

Our E-Safety Policy has been written by the school, building on government guidance. Changes will be made immediately if technological or other developments so require.

WHAT IS E-SAFETY?

E-Safety encompasses Internet technologies and electronic communications such as mobile phones. This policy 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. This policy operates in conjunction with other school policies including those for ICT, Behaviour, Anti-Bullying, PHSE and Child Protection.

TEACHING & LEARNING

WHY IS INTERNET USE IMPORTANT?

The purpose of Internet use in school is to raise educational standards, to promote child achievement, to support the professional work of staff and to enhance the school's management functions. Internet use is a part of the curriculum and a necessary tool for learning. Internet access is an entitlement for Children who show a responsible and mature approach to its use. The school has a duty to provide Children with quality Internet access as part of their learning experience. Children use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

HOW DOES THE INTERNET BENEFIT EDUCATION?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries
- Access to experts in many fields for children and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across support services (Wolverhampton LA Engage), professional associations (ISI, IAPS) and between colleagues
- Improved access to technical support including remote management of networks (Concero) and automatic system updates
- Access to tools of direct communication, including email
- Exchange of curriculum and administration data with ISI and DfE

HOW CAN INTERNET USE ENHANCE EDUCATION?

- The school Internet access will be designed expressly for child use and will include filtering appropriate to the age of children

- Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of children
- Staff should guide children in on-line activities that will support the learning outcomes planned for the children' age and maturity
- Children will be educated in the effective use of the Internet in research

HOW WILL CHILDREN LEARN TO EALUATE INTERNET CONTENT?

- If members of staff discover unsuitable sites the URL (address) and content must be reported to the Internet Service Provider via Concero
- Key Stage 2 children should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

COPYRIGHT

Under UK law, copyright material published on the internet will generally be protected in the same way as material in other media. Each web page may contain different copyrights if it contains text, music and graphics. Many websites will include a copyright statement setting out exactly the way in which materials on the site may be used.

Staff working with children need to consider copyright of material they use, and they should educate children on copyright issues.

The following sites are child-friendly and have copyright permissions for educational use:

- **ARKive Education**: This provides wildlife videos, images and fact files for classroom use on a wide range of science, ICT and literacy projects
- **Pics4Learning**: This copyright-friendly image library consists of thousands of images donated by teachers, students and amateur photographers
- **VADS** (Visual Arts Data Service) online resource: This online resource for visual arts provides over 100,000 digital images, free for use in education

MANAGING INFORMATION SERVICES

HOW WILL OUR ICT SYSTEM SECURITY BE MAINTAINED?

- The school ICT systems will be reviewed regularly with regard to security by Concero
- Virus protection will be installed and updated regularly by Concero
- Files held on the school's network will be regularly checked
- Concero will ensure that the system has the capacity to take increased traffic caused by Internet use
- The use of user logins and passwords to access the school network will be enforced

HOW WILL E-MAIL BE MANAGED?

- Each member of staff has access to their own school-based email account, which is specific to their system login
- School based email accounts should not be used for social e-mail

- The forwarding of chain messages is not permitted

HOW SHOULD WEBSITE CONTENT BE MANAGED?

- The point of contact on the website will be the school address, school e-mail and telephone number. Staff or children' personal information will not be published
- The Headmistress will take overall editorial responsibility and ensure content is accurate and appropriate on all pages directly related to the day-to-day workings of the school
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained

CAN CHILDREN' IMAGES OR WORK BE PUBLISHED?

- Images which include children will be selected carefully and only those children whose parental permission has been given will be used
- Written permission is given by parents' consent form when children start in TOTS and when new children join. This data is held by Ms Kempson, School Secretary
- Children' full names will not be used on the Website when associated with photographs, or in any way which may be to the detriment of children
- Child photographs will immediately be removed from the school Website upon request from parents, or other appropriate request

HOW WILL SOCIAL NETWORKING AND PERSONAL PUBLISHING BE MANAGED?

- The school will block access to social networking sites for children
- Children will be advised that Facebook Accounts should not be held under the age of 13 years old
- Children 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, IM and e-mail addresses, full names of friends, specific interests and clubs etc
- Children 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
- Children should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Children should be encouraged to invite known friends only and deny access to others

HOW WILL FILTERING BE MANAGED?

- Concero will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Any material that the school believes is illegal must be referred to Concero and CEOP (Child Exploitation & Online Protection)
- Filtering strategies will be selected by Concero in discussion with the school where appropriate. Where possible, the filtering strategy will be selected to suit the age and curriculum requirements of children

HOW CAN EMERGING INTERNET USES BE MANAGED?

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

HOW SHOULD PERSONAL DATA BE PROTECTED?

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

HOW WILL INTERNET ACCESS BE AUTHORISED?

- All staff and children will initially be granted access to the school's electronic communications
- Parents will be informed that children will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form when they join Newbridge Preparatory School
- Children will not be allowed to use computers with Internet unless they are directly supervised by a member of staff

HOW WILL THE RISKS BE ASSESSED?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for children. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and linked nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.

The following measures are in place:

Internet access at Newbridge Preparatory School is filtered by our Internet Service Provider (ISP) but ultimately, teachers, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. We also have a secondary filtering provided by a dedicated internet server/router. This provides additional filtering which allows the children to only view certain pages.

Posters in the Computing Room remind children how to keep safe on line.

WHAT ABOUT THE RISKS OF RADICALISATION?

The Government's Prevent Strategy and resources are well established and in many places well-coordinated, however this is not necessarily the case everywhere. It is the intention of the UK Safer Internet Centre to ensure that these risks and threats are considered for every child, right across the country, including places that have traditionally seen themselves as not being at risk – the Internet does not recognise these places and neither should we.

- For more information on PREVENT please follow this: https://www.gov.uk/government/policies/protecting-the-uk-against-terrorism/supportingpages/prevent
- For more information about the Home Office's radicalisation awareness training product Workshop to Raise Awareness of Prevent (WRAP) email WRAP@homeoffice.x.gsi.gov.uk

- If you have a concern about a child in respect of extremism and the support options are not available locally, talk to your LSCB police representative who will be able to discuss support options.
- To report suspected online terrorist content please follow this https://www.gov.uk/report-terrorism
- You can also refer content of concern directly to social media platforms - find out how: http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/safety-features

Teachers ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Newbridge Preparatory School has a suitable filtering is in place which is provided and monitored by Concero.

HOW WILL E-SAFETY COMPLAINTS BE HANDLED?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure. Any complaint about staff misuse must be referred to the Headmistress
- Children and parents will be informed of the complaints procedure
- Parents and children will need to work in partnership with staff to resolve issues
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies
- Sanctions available include: - interview/counselling by senior member of staff/class teacher/teaching assistants; - informing parents or carers; - removal of Internet or computer access for a period, which could prevent access to school work held on the system

HOW IS THE INTERNET USED ACROSS THE COMMUNITY?

- The school will liaise with local organisations to establish a common approach to e-safety
- The school will be sensitive to Internet related issues experienced by children out of school, e.g. social networking sites, and offer appropriate advice

CYBER BULLYING

HOW WILL CYBER BULLYING BE MANAGED?

Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF2007. Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyber bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

- Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on using the school Anti-bullying Policy and Procedures

- Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour
- There are clear procedures in place to support anyone in the school community affected by bullying and this includes cyber bullying
- All incidents of cyber bullying, as bullying, reported to the school will be recorded
- There will be clear procedures in place to investigate incidents or allegations of cyber bullying as a form of bullying
- Children, staff and parents/carers will be advised to keep a record of the bullying as evidence
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary
- Children, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's e-Safety ethos

Sanctions for those involved in cyber bullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content
- Internet access may be suspended at school for the user for a period of time
- Parent/carers of children will be informed
- The Police will be contacted if a criminal offence is suspected

CHILDRENS USE OF PERSONAL DEVICES

Electronic devices of any kind cannot be brought in to school by children. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

- If a child breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy
- Parents are advised to contact the school office

STAFF USE OF PERSONAL DEVICES

The use of mobile phones and other personal devices by staff in school will be decided by the school and covered in the school Acceptable Use of Mobile Phone Policies.

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity
- Staff will be issued with a school phone where contact with parents/carers is required
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances

- If members of staff have an educational reason to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of children and will only use work-provided equipment for this purpose
- If a member of staff breaches the school policy then disciplinary action may be taken.

ESAFETY QUALIFICATIONS

Mrs C. Northall (KS1) and Miss K. Hughes (KS2) have completed an EPICT course. The EPICT Esafety Certificated course enables educators to be confident in their knowledge of esafety threats, precautions and interventions. The course consisted of one half-day training session with, Alan Foster (Concero), followed by one assessed assignment. Both members of staff have been awarded a certificate and are fully EPICT accredited, a qualification which is recognised by **OFSTED**. For more information please visit: http://www.epict.co.uk/

PARENTAL INFORMATION

Provide workshops for parents to attend to help raise awareness

04/04/2013
SAF

Reviewed 04/04/2014
SAF
Reviewed 15/12/2015
SAF