Harewood Nursery School

E-Safety Policy

Harewood Nursery School E-Safety Policy 2018-19

Introduction

Harewood Nursery School fully recognises the contribution it can make to protect children and support them in school. The aim of this policy is to safeguard and promote our children's safe use of the internet and electronic communication technology. The internet and other technologies have an important role in the learning and teaching processes however, we feel it is important to balance those benefits with an awareness of the potential risks. This policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, children and parents and carers in their online experiences.

The school acknowledges e-safety and e-security as important issues for our school community and has made a considered attempt to embed e-safety into our teaching and learning using technology and have considered the wider implications of e-safety beyond classroom practice such as security and data.

This policy applies to the whole school community including, school governors, all staff employed directly or indirectly by the school and all children. The Headteacher and school governors will ensure that any relevant or new legislation that may impact upon the provision for e-safety within school will be reflected within this policy.

What is E-Safety?

E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act upon them. Safeguarding and promoting the welfare of all children is embedded in the culture of the school and within everyday practices and procedures.

All staff have a responsibility to support e-safety practises in school. Concerns related to child protection will be dealt with in accordance with the school's Safeguarding Policy and should be reported to designated safeguarding lead persons.

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils
- A comprehensive, agreed and implemented e-Safety Policy
- Secure, filtered broadband
- The use of e-safety control software monitoring system which monitors and captures inappropriate words or web sites used

Aims:

- To set out the key principles expected of all members of the school community with respect to the use of ICT-based technologies
- To safeguard and protect the children and staff

- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- To minimise the risk of misplaced or malicious allegations made against adults who work with children

Roles and Responsibilities

We believe that e-Safeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching.

The Governing Body of the school are responsible for the approval of this e-safety policy and for reviewing the effectiveness of the policy. This is carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

The Headteacher will:

- Ensure all staff are included in e-safety training. Staff must understand that misuse of the internet may lead to disciplinary action and possible dismissal
- Ensure that all temporary staff and volunteers including students are made aware of the school's e-safety policy arrangements
- Be the first point of contact for all e-safety matters; alongside the deputy DSLs
- Take day-to-day responsibility for e-safety within school
- Have a leading role in establishing and reviewing the school e-safety policy and procedures
- Communicate regularly with the designated Safeguarding governor
- Ensure that e-safety is promoted to parents and carers
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- Ensure that an e-safety incident log is kept up to date
- Ensure that the school Acceptable Use policy is current and pertinent
- Ensure that the Designated Leaders for Safeguarding are trained in e-safety issues and are aware of the potential for serious child protection issues which could arise from; sharing of personal data, inappropriate online contact with adults and strangers, potential or actual incidents of grooming, cyber bullying
- Take ultimate responsibility for e-safety provision including for all members of the school community

School Staff responsibilities include:

- To read, understand and help promote the school's e-safety policy
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the Headteacher

- To develop and maintain an awareness of current e-safety issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with parents should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed e-safety messages in learning activities across all areas of the EYES
- To supervise and guide children carefully when engaged in learning activities involving technology
- To ensure that children are aware within the scope of their understanding of how to use technology safely
- To be aware of e-safety issues related to the use of mobile phones, cameras and handheld devices
- To maintain a professional level of conduct in personal use of technology at all times

The ICT support technicians (MINT) will:

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others on relevant changes

Parents and Carers will:

- Be informed of the schools e-safety policy which can be accessed via the school website
- Will be informed of any issues concerning the internet / websites / games as soon as possible
- Will support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school
- Will be offered advice on filtering systems and appropriate educational and leisure activities including responsible use of the internet
- Will be provided with up to date and relevant information through the 'Safer Schools' App
- Will be expected to comply with the school's policy on the use of photographic and video images outside of school

Responsibilities of the children:

- To begin to be aware of benefits and risks of using the internet and other technologies both at school and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home
- To know who they can talk to about using the internet; e.g. staff, parent, carers

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for our children but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our children's lives and we believe we have a duty to help prepare our children to safely benefit from the opportunities the internet brings. In order to do this we will:

- Ensure that e-safety is an integral thread throughout our school.
- Celebrate and promote e-safety through group activities, including promoting Safer Internet Day
- Ensure that any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas
- Ensure children will be shown how to use a range of age-appropriate online tools in a safe and effective way
- Ensure staff model safe and responsible behaviour in their own use of technology
- Ensure that when searching the internet for information, children will be guided to use age-appropriate search engines
- Ensure all use will be monitored and children will be reminded of what to do if they come across unsuitable content
- Ensure all children are made aware of where to find help if they experience problems when using the internet and related technologies; i.e. parent or carer or member of staff

Managing Passwords

Passwords are an important part of computer security, they are a form of authenticating a user against a given username. Staff are reminded that usernames and passwords should not be shared with other members of staff. All staff are forced to change their passwords periodically under the guidance of the ICT Support technicians.

Managing Internet Access

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.

- The school internet access is designed expressively for educational use and will include filtering appropriate to the age of the children
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access
- Servers, workstations and other hardware and software will be kept updated as appropriate
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- All staff, volunteers and students will sign an Acceptable Use Policy provided by the school

- Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked

Managing email

- Incoming e-mails should be monitored and attachments should not be opened unless the author is known
- Access at school to external e-mail accounts may be blocked (at the discretion of the Headteacher)
- Staff sending any work related communications will always utilise a school email address (never a personal email account)
- Consideration will always be given to the types of content sent to external third parties at all times (e.g sending pupil information etc)
- Sensitive information should include encrypt in the subject part of the email so it is encrypted as an added security

Managing school website content

- Photographs of pupils will not be used without the written consent of the children's parents/carers
- The point of contact on the school website will be the school address, email and telephone number
- Staff or children's home information will never be published.
- The Headteacher will have overall editorial responsibility and ensure the content is accurate and appropriate

Filtering

- The school will work in partnership with parents/carers; the Local Authority, the DFE, the Internet Service Provider and MINT to ensure systems to protect pupils and staff are reviewed and improved regularly.
- All internet usage will be monitored for inappropriate use
- If staff or children discover unsuitable sites, the URL and content must be reported to the Headteacher
- Regular checks by MINT will ensure that the filtering methods selected are appropriate, effective and reasonable
- We filter out social media, such as Facebook
- Searched and web addresses are monitored and the ICT technicians will alert the Headteacher where there are concerns and prevent further access when new sites that are unblocked are found

Managing digital content Camera and images

Written permission form parents or carers will be obtained for the following areas before photographs of pupils are published. 1. On the school website 2. In display material that may be used around school 3. In display material that may be used off site 4. Recorded or transmitted on a video or via webcam in an educational conference 5. Media publications

Storage of images

Any photograph/video of children should be taken using school owned devices. All data images on a camera or internal storage should be removed on a regular basis.

Mobile Phones

Staff are allowed to bring mobile phones on to the school premises. These have to be stored in the staffroom in the lockers provided. Staff should make mobile communications in a safe place away from children and not during session times. Staff are not permitted to use their own personal phones for contacting children or their families within or outside of the setting in a professional capacity.

Social networking, social media and personal publishing

- Staff using social media websites will not bring school or their own professional status into disrepute
- Staff are accurately aware of the risks of adding pupils/parents as friends.
- Staff will not discuss any element of their professional lives or matters concerning Harewood Nursery school on social media sites
- The Headteacher will act upon anything they find on social media posted by staff or parents, which they feel would bring the school into disrepute, or children into danger

The school business manager as Data Protection Lead will:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged off' at the end of any session in which they are using personal data
- Ensure any email containing personal data will be encrypted
- Will ensure that data will be securely deleted from all devices, in line with the school Data Retention Policy once it has been transferred or its use is complete
- Will remind staff of their GDPR responsibilities eg not leaving personal and sensitive printed documents on printers within public areas of the school
- Ensure that when disposing of equipment all drives to be erased ensuring no sensitive information remains on the hard disk or storage of any kind
- Ensure any documents containing confidential information are shredded within school

Responding to issues of misuse

Staff:
It is hoped that all members of the school community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or very rarely through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents: If any apparent or actual misuse appears to

involve illegal activity ie. Child sexual abuse images, adult material which potentially breaches the Obscene Publications act, criminal racist material then the staff responsible will be subject to disciplinary and dealt with through the Local Area Designated Officer Procedures. If any staff member suspects illegal activity, it must be reported immediately to the Headteacher. The matter must not be discussed with other members of staff under any circumstances. If there is a breach of the e-safety Policy that is not considered illegal then the matter will be dealt with appropriately and proportionally.

Children:
All staff are responsible for ensuring children remain safe whilst using technology through ongoing teaching.

Dealing with complaints

Staff, parents and carers must know how to report incidents to the Headteacher. Concerns relating to Safeguarding must be dealt with through the School's Safeguarding Policy and Procedures. All e-safety complaints and incidents will be recorded in school, including any action taken.

The Headteacher will be responsible for dealing with complaints and any complaint concerning staff or children's misuse of the internet must be reported to the Headteacher immediately.

Through all these measures we hope that our children have a positive experience when using the internet safely and that they develop an awareness of IT as a useful tool and further develop their skills.

Monitoring and Reviewing

This policy is monitored by the Headteacher, who reports to the governors about the effectiveness of the policy on request. It will be reviewed appropriate to new legislation or to the needs of the school. Any changes will be disseminated to staff and governors.

Date for Review January 2020

Named Governor for Safeguarding, including E-Safety: Mrs Sarah Conway – Chair of Governors