Hoylandswaine Primary School

E-Safeguarding Policy
July 2015

Introduction

The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience. It is the duty of the school to ensure that every child and young person in its care is safe. E-Safeguarding encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. The purpose of internet use in school is to help raise educational standards and promote pupil achievement. This policy highlights the internet use to educate children and young people about the benefits and risks of using new technology and provide safeguards and awareness for users to enable them to control their online experiences.

This policy has been developed to ensure that all stakeholders and working together to safeguard and promote the welfare of children. E-Safeguarding is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of E-Safeguarding at all times, to know the required procedures and to act on them. Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures. All staff have a responsibility to support E-Safeguarding practices in school. Concerns related to child protection will be dealt with in accordance with the school's Safeguarding Policy and should be reported to the designated persons.

The policy is to be referenced alongside the safer use of the internet, data protection, social media, safeguarding, behaviour and anti-bullying policies.

Roles & Responsibilities

The SLT will (ensure):

- All staff are included in E-Safeguarding training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated Senior Member of Staff for E-Learning/Safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers including students are made aware of the school's E-Safeguarding Policy and arrangements.
- A commitment to E-Safeguarding is an integral part of the safer recruitment and selection process of staff and volunteers.
- A senior member of staff is designated as the Senior Information Risk Officer (SIRO) to assess the risk of the use of different types of technology and information data sets that are owned by the school.
- Develop and promote an E-Safeguarding culture within the school community.
- Support the E-Safeguarding Leader in their work.

The Governing Body of the school with ensure that:

- There is a senior member of the school's leadership team who is designated to take the lead on E-Learning/Safety within the school (Mr Damien Bond)
- There is a robust system for Incident reporting. Procedures are in place for dealing with breaches of E-Safety and security and are in line with Local Authority procedures (e-safety written log and electronic log)
- All staff and volunteers have access to appropriate ICT training.
- They have read, understand and contribute to and help promote the school's E-Safeguarding policies and guidance.
- Appropriate funding and resources are available for the school to implement their E-Safeguarding strategy.

The Designated Senior Member of Staff for E-Safeguarding will ensure:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.

- Provide support and training for staff, governors and volunteers on E-Safeguarding.
- All staff, governors and visitors read and sign the schools acceptable use agreement.
- All staff and volunteers understand and aware of the school's E-Safeguarding policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with the LA particularly where a wide area network is planned.
- E-Safeguarding education is embedded across the curriculum.
- E-Safeguarding is promoted to parents and carers.
- The Senior Information Risk Officer (SIRO) has carried out appropriate risk assessments dealing with the use of ICT equipment and technologies and the information data sets owned by the school.
- An E-Safeguarding incident log is kept up-to-date and regularly monitored/reviewed termly by the incident management team (E-Safeguarding coordinator, SIRO if different from the E-Safeguarding coordinator, ICT technician and where possible a designated member of the governing body).

Teachers and Support Staff will:

- Read, understand and help promote the school's E-Safeguarding policies and guidance.
- Read, understand and adhere to the school staff Acceptable use Policy (AUP).
- Develop and maintain an awareness of current E-Safeguarding issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed E-Safeguarding messages in learning activities where appropriate.
- Supervise children carefully when engaged in learning activities involving technology.
- Be aware of what to do if an E-Safeguarding incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.

Teaching & Learning

The internet is an important part of the statutory curriculum and a necessary tool for staff and children. The internet benefits education by allowing access to world-wide education resources. The school Internet access is designed expressly for child and educational use. All internet access shall be filtered for inappropriate images and websites in accordance with the local authority and Internet Watch Foundation (IWF) policies. Children are taught what Internet use is acceptable and what is not through the 'Rules for using the internet' posters. Clearly planned learning objectives for using the Internet are shared with the children before the session and pupils are taught how to safely search for internet content of all types (images, information, video, music, etc.) in order to further their learning. In Key Stage 1 pupils and staff have been educated on 'Hector the Protector' and the icon is available on every computer within school. Children are taught what to do if they access inappropriate material by clicking on the 'Hector' icon and waiting for a member of staff who will resolve the issue. In Key Stage 2 children are taught using the CEOP materials and the 'Cyber Café. If children access inappropriate material they inform a member of staff, who reports it to the E-Safeguarding Leader who subsequently informs the Headteacher.

The school will provide a series of specific E-Safety related lessons in every year as part of the Computing Curriculum / PSHCE curriculum / other lessons. We will celebrate and promote E-Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year. We will discuss, remind or raise relevant E-Safety messages with children routinely whenever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.

Managing Passwords

Passwords are an important part of computer security; they are a form of authenticating a user against a given username. At Hoylandswaine Primary School the decision has been made that pupils will use passwords as of September 2015 that will contain three characters and will be changed every 90 days.

- All staff are to change their passwords every 45 days under the guidance of the ICT Leader, consideration should be given to minimum password length and complexity, utilising both upper and lowercase letters, numbers and special characters.

Managing Internet Access

- The school will agree which users should and shouldn't have Internet access, and appropriate level of access and supervision they should receive.
- The school internet access id designed expressly for pupil use and will include filtering appropriate to the age of the children and young people.
- All users will sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
- Children will be taught what internet use is acceptable and what is not and be given clear objectives for internet use through the 'Rules for using the internet' posters. Staff will guide children in on-line activities that will support the learning outcomes planned for the child's age and maturity.
- Children will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening by clicking on 'Hector the Protector' and referring to 'Sid's rules'.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider (Barnsley Local Authority) via the E-Safeguarding Leader. Any incidents relating to unsuitable sites/content should be documented within the E-Safeguarding Incident Management log.

Managing E-Mail

- Children are not allowed personal e-mail addresses in school.
- Whole-class or group e-mail addresses will be used for communication with others.
- Incoming e-mail should be monitored by the class teacher and attachments should not be opened unless the author is known.
- Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone as introduced by 'Hector the Protector' and 'Cyber Café'.
- Access in school to external personal e-mail accounts may be blocked (At the discretion of the Headteacher and designated E-Safeguarding lead).
- Staff sending any work related to communications will always utilise a school e-mail address (Never a personal e-mail account) Consideration will be given to the types of content sent to external third parties at all times (e.g. sending pupil information, etc.)

Managing School Website Content

- Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.
- Photographs of pupils will not be used without the written consent of the pupil's parents/carers.
- The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupil's home information will not be published.
- The Headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.
- The website will comply with the school's guidelines for publications and parents/carers will be informed of the school's policy on image taking and publishing.
- Use of site photographs will be carefully selected so that pupils cannot be identified or their image misused. The names of pupils will not be used on the website, particularly in association with any photographs.
- Work will only be used on the website with the permission of the pupil and their parents/carers.
- The copyright of all materials must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Filtering

- The school will work in partnership with parents/carers; the Local Authority, the DFE and the Internet Service Provider 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 E-Safeguarding Leader.
- Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk) and the local authority.
- Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable.
- The level of filtering and content available will be selected by the school in conjunction with the LA and will be age and curriculum appropriate.

Use of Mobile Devices

- Children are not permitted to bring into school mobile devices such as mobile phones and handheld games. Staff have the right to confiscate these.
- Staff are allowed to bring mobile phones onto the school premises. These have to be stored with personal belongings out of reach of children. Staff under no circumstances should be using their mobile phones during lesson times especially when working with children. Staff are not permitted to take photographs of children on their mobile phones for security reasons.
- 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.

Camera & Images

- Any photographs/video of children should be taken using school owned devices. All data images situated on camera internal storage should be removed on a regular basis.
- For further information see the Data Protection Policy.

Protecting Personal Data

The school will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998 (see the end of this policy).

- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission of the Headteacher, and without ensuring such data is kept secure.
- For further information see the Data Protection Policy.

Social Networking, Social Media and Personal Publishing

- Staff using social media websites such as Facebook and Twitter will not bring the school or their own professional status into disrepute.
- Guidance on security settings for Facebook and other sites is available from Mr Damien Bond and instructions should be followed in line with the schools Social Media Policy.
- Staff should be aware that it is prohibited to add children/parents as friends.
- Staff will not discuss professional matters on social media sites.
- Through the work of 'Thinkuknow' staff will teach children the importance of protecting data.

Dealing with Complaints

- Staff, children and parents/carers must know to report incidents to the Headteacher. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding Policy and Procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- All e-safety complaints and incidents will be recorded by the school, including any actions taken.
- The school's designated person for E-Safeguarding (Mr Damien Bond) will be responsible for dealing with complaints and any complaint concerning staff or child misuse of the internet must be reported to the Headteacher immediately. Any misuse will be recorded electronically.
- Parents/carers and children will work in partnership with the school staff to resolve any issues.
- Sanctions for misuse for pupils may include any or all of the following:
  - Discussions with the Headteacher
  - Informing parents/carers
  - Removal of internet access for a specified period of time

Parent and Carers Support

- Parents/carers will be informed of the school's Safer Use of Internet Policy which can be accessed via the school website.
- Any issues concerning the internet will be handled sensitively to inform parents/carers without undue alarm.
- Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers.
- A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.
- Parents/carers will be expected to agree and sign the home/school agreement which clearly states the use of photographic and video images outside of school.

Through all these measures we hope that children have a positive experience when using the Internet and that ICT can be used as a tool to further develop and teach vital life skills allowing children to make a positive contribution.

Data Protection Act 1998

School collects data in order to meet its statutory responsibilities for the provision of education to children in accordance with the requirements of the Education Act 1996 and The School Standards and Framework Act 1998. Some of this data will be shared with Barnsley Metropolitan Borough Council and may be shared with other agencies that are involved in the health and welfare of school children. Please be aware that personal data is also covered by the Data Protection Act 1998 whereby you as an individual may be liable if you disclose personal data inappropriately. Please see the school's Data Protection policy.

Inclusion

The policy will be applied to all pupils. We welcome our general responsibilities under the Disability Equality Duty by promoting equal opportunities, eliminating discrimination and improving access to learning for disabled people. In order to comply with the requirements of the Equality Act 2010 we will make reasonable adjustments to ensure all stakeholders understand and can follow this policy. We will actively seek to remove any barriers to learning and participation that may hinder or exclude individuals or groups of children.

Monitoring and Review

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

This policy will be reviewed in July 2017

Signed ____________________________Headteacher Date ________________

Signed ____________________________Chair of Governors Date ________________