

Houghton Primary School

The purpose of this policy is to outline the safeguarding measures in place for adults and children at Houghton Primary School. It explains how we aim to protect and educate pupils and staff in their use of technology and the mechanisms which exist to intervene and support any incident where appropriate. Our key aim is to protect and educate children against the range of e-safety issues which can be best categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material
- contact: being subjected to harmful online interaction with other users
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

At Houghton School we feel that the most successful approach lies in equipping our pupils to become confident, discerning and resilient users of technology. This is best achieved through strong partnership with parents.

We aim to involve parents through:

- Inviting parents to regular parent information evenings.
- Parent access to e-safety materials stored on the designated e-safety page on the school's website.
- Parental involvement with children through the setting of e-safety competitions and home learning.

Our E-safety policy is systematically reviewed to ensure that it has a positive impact on pupils' knowledge and understanding. All teaching and non-teaching staff in the school community take part in regular e-safety training.

Rationale

At Houghton School believe that the use of information and communication technologies in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to raise educational standards and promote

E Safety Policy

pupil achievement. Yet at the same time we recognise that the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

Content

- exposure to inappropriate content, including online pornography; ignoring age ratings in games (exposure to violence, often associated with racist language); and substance abuse
- lifestyle websites, for example pro-anorexia, self-harm or suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content.

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film).

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the school. For example, school and personal data being entered on web/social networking sites, fraudulent email traps and cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision, to manage the risk and deal with any threat to safety.

Teaching and Learning Using Online Technologies

The internet is a part of everyday life for education, business and social interaction. Benefits of using online technologies in education include:

- Access to world-wide educational resources;
- Access to experts who would otherwise be unavailable;
- Access to anytime, anywhere learning; and
- Collaboration across schools, networks of schools and services.

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. At Houghton we believe that a comprehensive programme of E-Safety education is vital for developing our pupils' ability to use technologies safely. This is achieved using a combination of discrete and embedded activities drawn from a selection of appropriate materials which build progressively through the school.

We believe that just as children learn how to swim by going to a swimming pool so they will learn safe, life-long online behaviours by accessing and using the internet. Members of staff constantly monitor pupils' use of the internet and other technologies. Our programme for E-Safety education is evidenced in teachers' planning either as discrete or embedded activities.

Messages involving risks, rules and responsibilities are taught and/or reinforced as detailed in the school's Acceptable Use Policies.

Technology In Our School

The school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service. [E2BN's Protex web filtering system received full Becta (British Educational Communications and Technology Agency) accreditation in 2007 by blocking over 90% of all inappropriate material. E2BN also manage a distributed caching service which is integrated with the web filtering service. Ref: E2BN Website] This helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. If/when they do, the school's Acceptable Use Policies and E-Safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

Technologies regularly used by pupils and adult stakeholders include:

Staff:

- Laptops and netbooks
- Tablet devices
- Cameras and video cameras
- Internet, E-mail, central hosting including access to SIMS and confidential pupil information.

Pupils:

- Netbooks
- Tablet devices
- Cameras and video cameras
- Internet,
- Other peripherals such as programmable toys, dataloggers, control technology equipment.

Others on school premises:

- Limited access to school systems such as filtered internet access using a visitor login.

Whilst we recognise the benefits of individual pupil logins to our school network, we prefer to use year group logins for ease of access. All members of staff have individual, password protected logins to the school network and visitors to the school can access part of the network using a generic visitor login and password. The school's network can be accessed using a wireless connection, however this is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office. School staff and pupils are not permitted to connect personal devices to the school's wireless network and the wireless key is not given to visitors to the school.

The E-Safety Curriculum

In line with recommendations in the E-Safety briefing for Section 5 Ofsted Inspectors (April 2014) we have planned a range of age-related teaching and learning opportunities to help our pupils to become safe and responsible users of new technologies. These opportunities include:

- Specific activities during e- safety week including e- safety assemblies

Houghton Primary School

- Age-related classroom activities using the ThinkUKnow materials
- Related work in PSHE lessons
- Posters and reminders in and around the school
- Competitions and home learning opportunities.

Safeguarding Children Online

Houghton primary recognises that different users will be expected to use the school's technology systems in different ways – appropriate to their age or role in school. We acknowledge the need to equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.

The school has published Acceptable Use Policies for pupils and staff who sign to indicate their acceptance of our AUPs and relevant sanctions which will be applied should rules be broken.

Any known or suspicious online misuse or problem will be reported to the designated E-Safety coordinator (Mrs. Frances Smith) for investigation/action/sanctions.

Responding to Incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an E-Safety incident occurs or they suspect a child is at risk through their use of technology. It is important that responses to E-Safety incidents are consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.

If an E-Safety incident occurs, we will follow our agreed procedures for dealing with incidents including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school's AUPs). Where we suspect that an incident may constitute a child protection issue, the usual child protection procedures will be followed.

Dealing with Incidents and Seeking Help

If a concern is raised, refer immediately to the designated person for child e-protection. It is their responsibility to:

E Safety Policy

Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator.

Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If in doubt they should consult the Education Child Protection Service helpline.

Step 3: Ensure that the incident is documented using the children protect incident logging form.

Depending on the judgements made at steps 1 and 2 the following actions should be taken:

Staff Instigator: Follow the standard procedures for managing allegations against a member of staff.

Staff Victim: Seek advice from EPM and/or Educational Child Protection Service.

Illegal activity involving a child: Refer directly to Cambridgeshire Constabulary – 0845 456 4564 – make clear that it is a child protection issue.

Inappropriate activity involving a child: Follow standard child protection procedures. If unsure seek advice from Education Child Protection Service helpline.

Equally, if the incident involves or leads to an allegation against a member of staff, the school will follow the agreed procedures for dealing with any allegation against a member of staff.

Review

This policy has been adopted by the staff and governors for implementation in September 2015.

It will be reviewed every two years, or sooner if required in line with other safeguarding policies and procedures.

Next review: Summer 2017