St Mary Magdalene C of E Primary School

E-Safety Policy

Children interact with new technologies such as mobile phones and the Internet on a daily basis. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place children and young people in danger.

'At St Mary Magdalene C of E Primary School we are committed to ensuring that all of our children and staff are safe and have the confidence, enthusiasm and knowledge to use ICT as a 21st century learning tool. However as a church school we want children to embrace new technologies but live their lives safely through Christian values'

Contents

1. Roles and responsibilities

Responsibilities: e-safety coordinator

Our e-safety coordinator is the person responsible to the head teacher and governors for the day to day issues relating to e-safety. The e-safety coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- receives appropriate training and support to fulfil their role effectively
- has responsibility for blocking / unblocking internet sites in the school's filtering system / passing on requests for blocking / un blocking to the ICT Helpdesk
- maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices
- Has received accredited training from Child exploitation and online protection (CEOP)
- Current named e-safety coordinator is Sarah Sedgwick

Responsibilities: head teacher

- The head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator
- The head teacher and another member of the senior management team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- E-safety issues are embedded in the curriculum and other school activities.

Responsibilities of parents

- Make sure that they allow children safe access to the internet when they are at home and that that they are aware of when and how children are accessing the internet.
- Parents report to school any issues involving cyber bullying or inappropriate internet use to school so correct behaviour can be reinforced during PSHME or ICT lessons.
- Read the e-safety newsletter sent home and keep up to date with e-safety changes reported by the school.

Responsibilities of the children

- Take part in and listen to e-safety lessons taking on board how to stay safe.
- Report any e-safety concerns to parents and teachers
- Know how to report any concerns via the CEOP button.
- Be able to explain to others how they are able to access the internet and communicate this to parents and staff.

2. Technologies

ICT in the 21st century has an all encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current emerging technologies used in school as well as outside school include:

- the internet
- email
- instant messaging often using simple web cameras
- blogs (an online interactive diary)
- Pod casting (radio/audio broadcasts downloaded to a computer or MP4 player.
- Social networking sights including facebook, twitter, my space and bebo.
- Chat rooms
- Gaming sites
- Music download sites
- Mobile phones with camera and video functionality
- Mobil technology (e.g. games consoles) that are internet ready.
- Smart phones with e-mail, web functionality and cut down 'office' applications.
- Ipads.

3. Communication

How will the policy be introduced to the children?

1) Termly key stage assemblies discussing updates to e-safety and how it impacts what ICT children are using in school and at home.
2) An e-safety training program will be introduced to raise to awareness and importance of safe and responsible internet use.
3) Children will receive 1 hour e-safety lesson each half term from year 1 – year 6.
   - This will be achieved by following the lesson modules on the www.thinkyouknow.co.uk website, which is maintained by CEOP.
4) Updated information on the E-safety display board.
5) Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon.

How will it be introduced to staff?

1) Staff will receive yearly updated training either through the LA or the e-safety co-ordinator.
   - This will include ways on how to teach children to be safe on the internet as well as protecting themselves and their privacy when using social networking sites such as facebook.
2) Staff will be informed by the e-safety coordinator procedures to follow in the case of an e-safety issue.
3) Staff will be given access to e-safety lesson plans and resources to complete 1 hour lesson each

term.

How will parents be introduced?

1) Parents will receive an e-safety news letter each term detailing methods on how to ensure children remain safe when using the internet at home.
2) A yearly e-safety meeting will take place where e-safety coordinator will provide advice on filtering systems and update on any e-safety issues which we have been informed of.

4. Computing security system

1. School computing systems security is reviewed regularly.

2. The Security of the schools information systems is reviewed regularly by the ICT technician (Concero), Open Hive and Computing leader.

3. Virus protection is updated regularly by the Network Manager and any faults reported immediately.

4. Security strategies are discussed with the Local Authority and Network Manager.

Managing filtering

1. The school works with its Network Manager and the LA to ensure systems to protect pupils are reviewed and improved.

2. If staff or pupils come across unsuitable on-line materials, the site is reported to the e-Safety Coordinator.

3. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

5. Authorising Internet access

1. All staff must read and sign the "Acceptable Use Policy" before using any school ICT resource.

2. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

3. At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

4. Parents will be asked to sign and return a consent form.

5. Any person not directly employed by the school will be asked to sign an "acceptable use of school ICT resources" before being allowed to access the internet from the school site.

6. Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

The school regularly audits Computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

7. Handling e-safety complaints

1. Complaints of Internet misuse is dealt with by a senior member of staff.

2. Any complaint about staff misuse must be referred to the head teacher.

3. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

4. Pupils and parents will be informed of the complaints procedure (see schools complaints policy)

5. Pupils and parents will be informed of consequences for pupils misusing the Internet.

9. What to do if there is a sudden example of inappropriate content on a computer in school

- If it is a case of inappropriate content being accessed or downloaded by a member of staff please comply with the following procedure.
  1) Turn off the monitor so the images cannot be seen. Do not turn off the computer.
  2) Do not try and remove the images or look to see where they came from.
  3) Inform e-safety coordinator and head teacher ASAP.
  4) Depending on the nature of the content Head teacher / e-safety coordinator to report the issue to the police.
  5) E-safety coordinator to inform Sandwell broadband.

- If it is a case of inappropriate content breaching Sandwell broadband filtering system please comply with the following procedure.

1) Turn off the monitor so the images cannot be seen. Do not turn off the computer.
2) Do not try and remove the images or look to see where they came from.
3) Inform e-safety coordinator ASAP.
4) E-safety coordinator to inform Sandwell broadband and report the website.
5) Sandwell broadband will filter the site

Review Date: July 2017