Excellence in E-Safety at Benjamin Adlard School

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

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

However, 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:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' knowledge to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school aims to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

E-Safety Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Anthem Trust:

The Trust are responsible for the writing of the E-Safety Policy. The Headteacher reports any e-safety incidents to them. IT Co-ordinators have set up Smoothwall Web Filter which sends daily emails to the Safeguarding Team. (Headteacher, DSL and DDSL)

We have in place web-filtering that blocks access to social media sites, chat rooms, online gaming sites and certain video hosting websites that do not have an internal filtering system.

Headteacher and Senior Leaders:

The Headteacher are responsible for ensuring that the Computing Co-ordinator and other relevant staff receive suitable CPD training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Headteacher and Senior Management are aware of the procedures to be followed in the event of a serious e- safety allegation being made against a member of staff.

Designated Safeguarding Lead

Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.

Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

Provide training and advice for staff

Liaise with school's ICT technical staff from Ark, which is provided under contract

Attends relevant meetings.

School Network Provider:

Ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack as well as off- site access

That the school meets the e-safety technical requirements

That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

They 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 as relevant

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

They have an up to date awareness of e-safety matters and attend staff training

They report any suspected misuse or problem to the Safeguarding Team or Headteacher for investigation

Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

They monitor ICT activity in lessons, extracurricular and extended schools activities

They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are place for dealing with any unsuitable material that is found in internet searches. This is highly unlikely due to the school's filtering policy but any breach should be reported immediately to the Headteacher or Safeguarding Team.

Designated Safeguarding Leads:

The Designated Safeguarding Leads (DSLs) should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

The DSL/DDSL ensure all school staff are trained in identifying E-safety risks and how to respond to them.

Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.

Pupils:

Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Will be expected to know and understand school policies on the use of mobile phones.

They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will therefore take every available opportunity to help parents understand these issues through parents' evenings, letters and the website.

Internet

The school internet access will be designed expressly for pupils use including appropriate content filtering.

Pupils will be given clear objectives for internet use and taught what use is acceptable and what is not.

Pupils will be educated in the effective use of the internet to research. Including the skills of knowledge location, retrieval and evaluation.

Social Networking

Social networking Internet sites provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

Use of social networking sites in the school is not allowed and will be blocked/filtered.

Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.

All staff are advised not to have contact with parents and children on any social networking site.

Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites.

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/ precaution use. These are handed to the class teacher at 8:50am and collected at the end of the day.

Staff should not use mobile phones to contact parents/guardians. School Staff will always use the school phone to contact parents/guardians.

The sending of abusive or inappropriate text message is forbidden.

Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom or on the playground.

Staff may use their mobile phones for personal use in the staffroom during the lunch period or before/after school.

Digital/Video Cameras

Pictures, videos and sound are not directly connected to the internet but images are easily transferred.

Pupils will not use digital cameras, mobile phones or video equipment as school unless specifically authorised by staff.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.

Staff are allowed to take digital/video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Staff will ensure that parent photograph permissions are followed in relation to publication and use of these images.

Those images should only be taken on school equipment, the personal equipment of staff can be used but only if other devices are unavailable. These images must be deleted by the end of the day.

Care should be taken when taking digital/video images that pupils are dressed appropriately and are not participating in activities that put them at risk or bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission

Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images

Pupils' full names will not be used anywhere on a website, particularly in association with images.

Permission from parents or carers will be obtained before photographs of pupils are published on the school website, social media or Trust advertising.

The Headteacher or nominee will inform parents/carers and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.

School Website

The school website is a valuable source of information for parents and potential parents.

Contact details on the website will be the school address, email, telephone and fax numbers.

Staff and pupils' personal information will not be published.

The Headteacher will take overall editorial responsibility and ensure the content is accurate and appropriate.

Photographs and videos that include pupils will be selected carefully and will adhere to parental photograph permissions completed on admission.

Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Consent from parents will be obtained before photographs of pupils are published on the school website.

Parents may upload pictures of their own children on to social networking sites. It cannot include other pupils.

Information System Security

School ICT systems capacity and security will be reviewed regularly.

Virus protection will be installed and updated regularly.

E-safety will be discussed with Anthem IT and Ark and those arrangements incorporated in our agreement with them.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school will audit ICT use to establish if the e-safety is adequate and appropriate.

Prevent Statement

The counter-terrorism and security bill was granted royal assent on 21 February 2015, which places a statutory duty on named organisations, including schools, to have due regard towards the need to prevent people being drawn into terrorism.

The most important part of this security bill is 'keeping pupils safe from the danger of radicalisation and extremism'.

The internet provides children and young people with access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their message. The filtering systems used at Benjamin Adlard Primary School block inappropriate content, including extremist content. Where staff or pupils find unlocked extremist content they must report it to the Senior Leadership Team.

Cyber Bullying

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils both in and outside school. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and unintended involvement an increased risk. Benjamin Adlard Primary School have a range of strategies and policies to prevent online bullying, outlined in various sections above.

No access to mobile phones nor public chat-rooms, Instant Messaging services on devices.

Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources. Specific education and training on cyber bullying (understanding what behaviour constitutes cyberbullying and its impact, how to handle concerns and report incidents) may be given as part of an annual Anti-bullying Week and E-safety Events.

Pupils are encouraged to discuss any concerns or worries they have about online bullying and harassment with their teachers or the Safeguarding Team.

Pupils are informed on how to report cyber bullying both directly within the platform they are on, and to school.

Complaints of cyber bullying are dealt with in accordance with our Anti-bullying Policy and if proven, recorded as Serious Incidents.

Complaints related to child protection are dealt with in accordance with school child protection procedures.

Handling e-safety complaints:

Complaints of internal internet misuse will be dealt with by the Headteacher.

Any complaint about staff misuse must be referred to the Headteacher.

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

Pupils and parents will be informed of the complaints procedure.

Pupils and E-safety .

Pupils will be informed that internet use will be monitored.

Pupils will be informed when they are in KS2 of the importance of being safe on social networking sites such as Snapchat. This will be strongly reinforced across all the year groups during computing lessons and all year groups look at different areas of safety through the digital learning lessons.

Staff and E-safety:

Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents and E-safety:

They will receive regular updates on e-safety via leaflets and information sent via Parentmail.

When issues are identified parents are invited in to have 1:1 support from IT co-ordinator.