ETTINGTON C of E PRIMARY SCHOOL

Reviewed December 2023

ETTINGTON
SCHOOL

Ettington Church of England
Primary School

Learning for Fullness of Life
Trust- Respect – Love

E Safety Policy

E-Safety Policy

Introduction
Building on the theological concepts that God created the earth and everything in it, we provide opportunities to appreciate God's creation of the world and how EVERYONE was made in God's image (Imago Dei) and loved, valued, celebrated and represented. As a school, we aspire to live out God's plan for all to flourish. We believe in providing our children with varied opportunities to use and develop the gifts and talents they have been blessed with, to ensure they embrace "Life in its fullness" (John 10:10).

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. This school e-safety policy should help to ensure safe and appropriate use.

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.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and safeguarding policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience 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 must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order 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 Policy

Our e-safety policy has been written following government guidelines. It has been agreed by all staff and approved by the Governing Board and can be found on the school website.

Development, Monitoring and Review

This e-safety policy was approved by the governing body and the implementation of the e-safety policy will be monitored by the computing Co-ordinator. Monitoring will take place annually.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

E-Safety Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the governors on the Curriculum Committee and the Safeguarding Governor receiving regular information about e-safety incidents and monitoring reports.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, through the day to day responsibility for e-safety will be delegated to the computing co-ordinator.
- The Headteacher/Senior Management are responsible for ensuring that the Computing Lead 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/Senior Management 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 Senior Management Team will receive regular monitoring reports from the Computing Lead.
- The Headteacher and Senior Management 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.

Computing 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 at Warwickshire County Council
- Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.
- Meets with the e-safety governor to discuss current issues and review incident logs
- Attends relevant meetings.

School Network Provider:

- 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 of the current e-safety policy and procedures
- They have read, understood and signed the school 'Staff Acceptable User Policy'
- They report any suspected misuse or problem to the Computing Lead or Headteacher for investigation
- Digital communications with pupils (VLE-Virtual Learning Environment) should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities- Use of Purple Mash scheme should ensure this is happening.
- Pupils follow the school e-safety and acceptable use policy
- 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.

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

Pupils:

- Are responsible for using the school ICT systems in accordance with the 'Pupil Acceptable Use Policy', which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- 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, digital cameras and hand-held devices. 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. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy

Teaching and Learning

The internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality internet access as part of their learning experience:

- The school internet access will be designed expressly for pupils use including appropriate content filtering.
- Pupils will, in the main, be using Purple Mash to access the IT curriculum. This is a safe domain for children to work.
- 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.
- As part of the new Computing (ICT) curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, our digital foot print and cyber-bullying.
- When children are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning.

World Wide Web

The internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupil discover unsuitable sites, the URL, time and content shall be reported to the teacher who will then record the incident on the e-safety log which will be stored on the laptop trolleys. The e-safety log will be reviewed termly by the Computing coordinator.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting it accuracy.
- The school will work with its technical support provider (RM) to ensure filtering systems are effective as possible. 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.

E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

- Pupils may only use the Purple Mash E-mail interface in Years 1 to 4 and then approved email accounts on the school system for Years 5 and 6.
- Pupils will only use the Purple Mash E-Mail interface for curriculum purposes and the approved e-mail accounts set up on the school system for Homework and Home Learning (TPS).
- Purple Mash Email facilities will be set up so firstly children will only have access to communicate with imaginary characters, then their teacher and finally pupils within their cohort (which will need approving by their class teacher).
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Should an email be sent to an external organisation then this should be done as a whole class, sent via the office and should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

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. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.
- Any queries, refer to the social media policy.

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 and telephone numbers.
- Staff and pupils’ personal information will not be published.

- The School Business Manager will take overall editorial responsibility and ensure the content is accurate and appropriate.
- 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. If the picture includes another child/children then it is their responsibility to gain permission from that child's parents.
- The governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

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 policy is adequate and that the implementation of the e-safety policy is 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 Ettington Primary School block inappropriate content, including extremist content. Where staff or pupils find unlocked extremist content they must report it to the Computing Lead or Head Teacher. Please refer to the Preventing Radicalisation Policy.

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. Ettington

Primary School have a range of strategies and policies to prevent online bullying, outlined in various sections of this Policy. These include:

- No access to mobile phones nor public chat-rooms whilst in school.
- 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.
- 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.
- 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 complaint's procedure.

Communication of Policy

Pupils and the E-safety Policy

- Rules for Internet access will be posted in all networked rooms.
- 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 msn. 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 the e-safety policy:

- All staff will be given the school e-safety policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents and the E-safety Policy:

- Parent's attention will be drawn to the School e-safety policy on the school website.
- They will receive regular updates on e-safety via leaflets and information sent via email.
- The parents will be encouraged to discuss code of conducts with their children before they are then asked to sign the 'Pupil Acceptable Use Policy'.

Review

This policy will be reviewed annually.

Virgin Media Internet Safety

When it comes to educating your kids about the internet, you might feel out of your depth, when they're learning, playing and chatting to friends on websites and apps you're unfamiliar with.

At Virgin Media O2, we want internet users of all ages to enjoy all the wonderful things the web has to offer, safely. That's why our experts have created a children's internet safety test to help build awareness for parents and children of all ages to ensure they are better protected online.

https://www.virginmedia.com/blog/online-safety/childrens-internet-safety-test/