Emmanuel Holcombe C of E Primary

E-Safety Policy

Vision Statement

Jesus came to give us life in all its fullness. Our vision is that through faith, family and friendship, each of us can grow in love and learning, being tolerant, having resilience and developing enquiring minds, so that we can all experience the abundance Jesus came to give us.

Mission statement

In our small, friendly school, everyone respects and cares for one another
In our community, church, home and school we work together to grown in faith and friendship
In our learning we encourage each individual to reach their potential to grow through skills, knowledge and understanding

Policy written: May 2020

Review date: May 2021

Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing and ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. Currently the apps and software children and young people are using both inside and outside of the classroom include:

- Websites
- Podcasting
- Coding
- Gaming
- Mobile devices
- Video & Multimedia

Whilst exciting and beneficial all users need to be aware of the range of risks associated with the use of these technologies.

At Emmanuel Holcombe we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school. Any visitors using their own devices within school, adhere to the schools Acceptable Use Agreement and this e-safety policy.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety co-ordinators at Emmanuel Holcombe school are computing coordinator; Mrs Clough, Headteacher; Mrs Bennett and Safeguarding co-ordinator;

This policy, supported by the school's acceptable use agreement, is to protect the interests and safety of the whole school community. It is linked to the following school policies: computing, child protection, behaviour, health and safety, anti-bullying and PHSE.

Responsibilities of the School Community

We believe that E-Safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The senior leadership team accepts the following responsibilities:

- The Headteacher will take ultimate responsibility for the E-Safety of the school community
- Identify a person (the E-Safety lead) to take day to day responsibility for E-Safety; provide them with training; monitor and support them in their work.
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure liaison with the Governors
- Develop and promote an E-Safety culture within the school community
- Ensure that all staff, pupils and other users agree to the Acceptable Use Policy and that new staff have E-Safety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to E-Safety
- Receive and regularly review E-Safety incident logs; ensure that the correct procedures are followed should an E-Safety incident occur in school and review incidents to see if further action is required with reference to the school's Behaviour and Safeguarding policies.

Responsibilities of the E-Safety Co-ordinator

- Promote an awareness and commitment to E-Safety throughout the school
- Be the first point of contact in school on all E-Safety matters
- Take day to day responsibility for E-Safety within the school
- Lead the school E-Safety team and/or liaise with technical staff on E-Safety issues
- Create and maintain E-Safety policies and procedures
- Develop an understanding of current E-Safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in E-Safety issues
- Ensure that E-Safety education is embedded across the curriculum
- Ensure that E-Safety is promoted to parents and carers
- Ensure that any person who is not a member of school staff, who makes use of the school ICT equipment in any context, is made aware of the Acceptable Use Policy
- Liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate, in accordance with the school's Safeguarding Policy
- Monitor and report on E-Safety issues to the E-Safety group, the Leadership team and the Safeguarding/E-Safety Governor as appropriate
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an E-Safety incident
- Ensure an E-Safety incident log is kept up to date
- Ensure that Good Practice Guides for E-Safety are displayed in classrooms and around the school
- To promote the positive use of modern technologies and the internet
- To ensure that the school E-Safety policy and Acceptable Use Policies are reviewed at prearranged time intervals.

Responsibilities of all Staff

- Read, understand and help promote the school's e-Safety policies and guidance
- Read, understand and adhere to the staff AUP
- Take responsibility for ensuring the safety of sensitive school data and information

- Develop and maintain an awareness of current E-Safety issues, legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Ensure that all digital communication with pupils is on a professional level and only through school-based systems, never through personal email, text, mobile phone social network or other online medium.
- Embed E-Safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all E-Safety incidents which occur in the appropriate log and/or to their line manager Respect, and share with pupils the feelings, rights, values and intellectual property of others in their use of technology in school and at home.

Additional Responsibilities of Technical Staff

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date
- Ensure that provision exists for misuse detection and malicious attack
- At the request of the Leadership team conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed
- Report any E-Safety-related issues that come to their attention to the E-Safety lead and/or senior leadership team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management
- Ensure that suitable access arrangements are in place for any external users of the schools ICT equipment
- Liaise with the Local Authority and others on E-Safety issues
- Document all technical procedures and review them for accuracy at appropriate intervals

- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster

Responsibilities of pupils

- Read, understand and adhere to the pupil AUP and follow all safe practice guidance
- Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all E-Safety incidents to appropriate members of staff
- Discuss E-Safety issues with family and friends in an open and honest way
- To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices
- To know, understand and follow school policies regarding Cyberbullying

Responsibilities of Parents and Carers

- Help and support the school in promoting E-Safety
- Read, understand and promote the pupil AUP with their children
- Discuss E-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images of pupils
- To agree to and sign the home-school agreement containing a statement regarding their personal use of social networks in relation the school:
- We will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's E-Safety policies and guidance as part of the school's overarching Safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-Safety awareness
- To have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data
- Ensure appropriate funding and resources are available for the school to implement their E-Safety strategy

Responsibilities of the Safeguarding Designated Person

- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information
- Be aware of and understand the risks to young people from online activities such as grooming for sexual exploitation, sexting, cyberbullying and others.
- Raise awareness of the particular issues which may arise for vulnerable pupils in the school's approach to E-Safety ensuring that staff know the correct child protection procedures to follow
- Responsibility of any external users of the school systems e.g. adult or community education groups; breakfast or afterschool club
- Take responsibility for liaising with the school on appropriate use of the school's IT equipment and internet, including providing an appropriate level of supervision where required
- Ensure that participants follow agreed Acceptable Use Procedures

E-safety in the curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for safety guidance to be given to the pupils on a regular and meaningful basis. We educate our children through our Computing Curriculum, Purple Mash and through activities completed on the e-AWARE website which helps us to assess children's online behaviour, identify risk, and raise e-safety awareness. Additionally, we continually look for new opportunities to promote E-Safety and teach e-safety through wider areas of the school such as, e-safety theme days.

- We provide opportunities within a range of curriculum areas to teach about E-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling, and activities as part of the ICT curriculum.
- Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- Students will have supervised access to Internet resources through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents re-check these sites and supervise this work.
- Our internet access is controlled through Bury LA's web filtering service.
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the E-Safety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up to date on all school machines.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. These are not to be used at any time whilst children are present.
- Any personal mobile devices have access to the internet via the schools WiFi guest network.
- The school is not responsible for the loss, damage or theft of any personal mobile device.

Managing email

- The use of email within school is an essential means of communication for staff.
- Pupils currently do not access individual email accounts within school.
- Staff must use the school's approved email system for any school business.
- Staff must inform the e-safety co-ordinator if they receive an offensive or inappropriate e-mail.

Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Creation of videos and photographs

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes School trips. School's own mobile devices must be used in this case.

Publishing pupil's images and work

- All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the school website, twitter account or mobile app.
- This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/ carers may withdraw or amend permission, in writing, at any time.
- Pupils' full names will not be published alongside their image and vice versa on the school website, twitter account, mobile app or any other school-based publicity materials.

Storage of Images

Images/ films of children are stored securely on the school server and / or teacher's individual school laptops.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- Follow password guidelines
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety rules.
- Users are provided with an individual network username
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

- If a password may have been compromised or someone else has become aware of the password the child or adult must report this to the E-Safety co-ordinator
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks
- Individual staff users must also make sure that workstations are not left unattended and are locked.

Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data.

Responding to E-Safety incidents/complaints

As a school we will take all reasonable precautions to ensure E-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor Bury LA can accept liability for material accessed, or any consequences of Internet access.

- Concerns relating to E-Safety should be made to the E-Safety co-ordinator. Any complaint about staff misuse must be referred to the Head teacher
- All users are aware of the procedures for reporting accidental access to inappropriate materials.
- The breach must be immediately reported to school's E-Safety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Head teacher/ Bury LA, LADO (Local Authority Designated Officer).
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Cyberbullying

Cyberbullying is the use of ICT, particularly mobile phones and the internet, deliberately to upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers have the power ‘to such an extent as is reasonable’ to regulate the conduct of pupils when they are off site’. Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

There are many types of cyber-bullying. Here are some of the more common:

- Text messages —that are threatening or cause discomfort - also included here is "bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology)
- Picture/video-clips via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.
- Mobile phone calls — silent calls or abusive messages; or stealing the victim’s phone and using it to harass others, to make them believe the victim is responsible.
- Emails — threatening or bullying emails, often sent using a pseudonym or somebody else’s name.
- Chatroom bullying — menacing or upsetting responses to children or young people when they are in web-based chatroom.
- Instant messaging (IM) — unpleasant messages sent while children conduct real-time conversations online using social media platforms.

The best way to deal with Cyberbullying is to prevent it happening in the first place and to have clear steps to take when responding to it.

Preventing Cyberbullying

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our E-Safety curriculum. They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.

- report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP).

Supporting the person being bullied

- Give reassurance that the person has done the right thing by telling someone and inform parents.
- Make sure the person knows not to retaliate or return the message.
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)
- Check the person knows how to prevent it from happening again e.g. blocking contacts,
- Changing contact details.

Investigating Incidents

All bullying incidents should be recorded and investigated in the Emmanuel Holcombe RC Primary School bullying incident log. We will:

- advise pupils and staff to try and keep a record of the bullying as evidence
- take steps to identify the bully, including looking at the school's systems, identifying and interviewing possible witnesses, and contacting the service provider and police if necessary.

The police will need to be involved to enable the service provider to look into the data of another user.

Working with the bully and sanctions

Once the bully is identified, steps should be taken to change their attitude and behaviour by educating them about the effects of Cyberbullying on others. Technology specific sanctions for pupil engaged in Cyberbullying behaviour could include limiting or refusing internet access for a period of time.

Factors to consider when determining the appropriate sanctions include:

- the impact on the victim: was the bully acting anonymously, was the material widely circulated and humiliating, how difficult was controlling the spread of material?
- the motivation of the bully: was the incident unintentional or retaliation to bullying behaviour from others?

Inappropriate contact with pupils via the internet

If it is found that there has been inappropriate contact with pupils via the internet, on official school systems, all evidence should be secured and preserved. The E-Safety coordinator and Headteacher should be informed immediately and steps taken in accordance with the school's Safeguarding policy.

Security, Data and Confidentiality

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- When accessing, amending and saving any data or information, relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the teacher, e-safety coordinators, Headteacher or Computing Coordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged, in the first instance, by PCedutech and then forwarded to the e-safety co-ordinator. Depending on the seriousness of the offence; investigation maybe carried out by the Headteacher or LA. Staff are aware that negligent use or deliberate misconduct could lead to disciplinary action.

Introducing the E-Safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- E-safety will be included more prominently in the Computing Curriculum.

Introducing staff and governors to the E-Safety policy

- All staff will be given the E-Safety policy and its application and importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.

- Staff/Governor training in safe and responsible Internet use and on our E-Safety policy will be provided as required.
- Teaching staff will be directed to be mindful of the teacher standards for professional conduct

Enlisting parents' support

At Emmanuel Holcombe, we believe that it is essential for parents/ carers to be fully involved with promoting E-Safety both in and outside of school. We regularly consult and discuss E-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

The school disseminates information to parents relating to E-Safety where appropriate in the form of:

- Information days/evenings
- Posters
- Website postings
- Newsletter items
- Parents/carers are asked to read through and sign acceptable use of ICT agreements on behalf of their child on admission to school
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- A partnership approach with parents will be encouraged. This includes parents' evenings/days with suggestions for safe home Internet use.
- Advice on filtering systems and educational activities that include safe use of the Internet will be made available to parents.

Equal Opportunities - Pupils with additional needs

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children.