Westcott Church of England School

E-Safety Policy

February 2024

This policy will be reviewed annually.

Background and Rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue. While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- 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 social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks.

We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Policy and Leadership

This section begins with an outline of the key people responsible for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school. It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of ICT.

Responsibilities: E-safety coordinator

Our e-safety coordinator is the head teacher.

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 ICT technical staff responsible for maintaining the school's ICT systems
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety development
- attends relevant meetings and committees of Governing Board
- reports regularly to Headteacher and Governing Board
- 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 / unblocking to the ICT Helpdesk
- maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices

Governors

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors (or a governors' subcommittee) receiving regular information about e-safety incidents and monitoring reports. A member of the governing body has taken on the role of Safeguarding governor which involves E-safety.

Headteacher

The headteacher is responsible for ensuring the safety (including e-safety) of members of the school community.

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 have read, understood and signed the school's Internet agreement
- they report any suspected misuse or problem to the E-Safety Co-ordinator • digital communications with students (Google Classroom/Meet) should be on a professional level and only carried out using official school systems
- e-safety is embedded in the curriculum and other school activities.

ICT technician

The ICT Technician is responsible for ensuring that:
- the school's ICT infrastructure is secure and is not open to misuse or malicious attack

- users may only access the school's networks through a properly enforced password protection policy
- shortcomings in the infrastructure are reported to the Headteacher so that appropriate action may be taken.

Pupils

- are responsible for using the school digital technology systems in accordance with safe practice
- 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 procedures on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyberbullying
- should understand the importance of adopting good online 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

Policy Development, Monitoring and Review

This e-safety policy has been developed by a working group made up of:

- School E-Safety Coordinator
- Head teacher / Senior Leaders
- Teachers
- Governors

Whole School approach and links to other policies

This policy has strong links to other school policies and documents as follows:

- Computing policy
- Staff Handbook
- Student handbook

How we strive to ensure that all individuals in school stay safe while using ICT

The e-safety policy constitutes a part of the Computing policy. Other documents and policies relating to e-safety:

PSHE: E-Safety has links to this – staying safe

Child Protection Policy: Safeguarding children electronically is an important aspect of E-Safety. The e-safety policy forms a part of the school's safeguarding policy

Behaviour: Linking to positive strategies for encouraging e-safety and sanctions for disregarding it.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:
• child sexual abuse images (illegal - The Protection of Children Act 1978)
• grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)
• possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008) • criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)
• pornography • promotion of any kind of discrimination
• promotion of racial or religious hatred
• threatening behaviour, including promotion of physical violence or mental harm
• any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.
Additionally, the following activities are also considered unacceptable on ICT equipment provided by the school:
• Using school systems to run a private business
• Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Buckinghamshire County Council and / or the school
• Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
• Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
• Creating or propagating computer viruses or other harmful files
• Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
• On-line gambling and non-educational gaming
• Use of personal social networking sites / profiles for non-educational purposes
• Staff may only access personal email accounts on school systems for emergency or extraordinary purposes (these may be blocked by filtering).
Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.
• Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Use of own devices in school

Staff and volunteers are allowed to bring personal mobile devices into school and for these to be left on but on silent. Mobile devices should not be brought out and used in the presence of any pupils at any time. In exceptional circumstances, for instance if the leader on a school trip needs to contact the school, use of a mobile device in the presence of pupils is permitted.

Pupils who bring mobile devices into school are to hand these into the School Office at the beginning of the school day. It can then be collected at the end of the school day. Watches worn by pupils should not have the capacity to send and receive messages or access the internet.

Reporting of e-safety breaches

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Listed below are the responses that will be made to any apparent or actual incidents of misuse:
Email/Google Account

- Access to email is provided for all users in school accessible via the web browser (internet Explorer) from their desktop. These official school email services may be regarded as safe and secure and are monitored.
- Staff should use only the school email services to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Pupils have access to a Google account with an individual account within their classroom for communication within school.

School Website

Our school uses the public facing website www.westcott.bucks.sch.uk for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information should not be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).
- Only pupil's first names are used on the website, and only then when necessary.
- Detailed calendars are not published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images: pupils' full names will not be used anywhere on a website or blog, and never in association with photographs

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Monitoring

- No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

E-Safety Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

- Users must immediately report, to their class teacher / e-safety coordinator – in accordance with the school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email. Use of digital and video images
- 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.
- Pupils must not take, use, share, publish or distribute images of others without their permission See also the following section for guidance on publication of photographs Use of web-based publication tools

E-Safety education will be provided in the following ways:

- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use google classroom.
- A planned e-safety programme should be provided as part of Computing, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Amongst others, we use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2)
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit. Information literacy
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:

Checking the likely validity of the URL (web address) o Cross checking references (can they find the same information on other sites)
Checking the pedigree of the compilers / owners of the website
• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
• Pupils are taught how to make best use of internet search engines to arrive at the information they require
• Amongst others, we use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2) Staff training It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.

It is expected that some staff will identify e-safety as a training need within the performance management process.

All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction

The E-Safety Coordinator will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority, the HSCB and others.

All teaching staff have been involved in the creation of this e-safety policy and are therefore aware of its content

The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an on-going basis.

Governor training

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in ICT, e-safety, health and safety or child protection. This may be offered by pParticipation in school training / information sessions for staff or parents The PHSE governor works closely with the e-safety coordinator and reports back to the full governing body.

Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). The school will therefore seek to provide information and awareness to parents and carers through:

- Workshops that focus on e-safety
- Letters and newsletters
- Parents evenings
- Reference to the parents materials on the Think U Know website via the school website (www.thinkuknow.co.uk) or others