Theale Church of England Primary School

e-Safety Policy

With technology usage even more prevalent at this time, e-safety is a vital part of children's life and education in today's ever-growing digital world and is rooted in their computing curriculum at our school.

As a school, we recognise the importance of assisting parents and children to improve their understanding of e-safety so that they can learn to support each other in using the internet and all digital media in a safe and secure way.

At School

The internet is an essential learning tool for our pupils as they grow up in the digital era. We strongly believe that they should develop familiarity and competence navigating the online world. However, we recognise that there are always concerns about children having access to undesirable materials and have taken positive steps to deal with this risk in school. All internet-capable devices accessible by pupils are subject to the filtering service provided by our ISP (RM).

Access to the internet is given to the children in adult-supervised settings. Use of the internet is strictly monitored by school staff and West Berkshire Council.

Pupils are also educated through the Computing curriculum on how to report any inappropriate material. A full e-Safety unit is taught each year from Years 1 to 6. All children in school are encouraged to follow the SMART rules to keep themselves safe online. An image of these rules can be found here.

At the start of the school year, we send home An Acceptable Usage policy to parent/carers for them to sign and agree to. We also ask every child in KS2 to sign an Acceptable Use Agreement policy so that we know they have read and understood our school's rules on staying safe when using devices and the internet and KS1 to sign an adapted version for our younger children.

Any breaches of this policy or e-safety concerns are taken extremely seriously, and steps are taken to prevent further occurrences – for more information on this, please read our e-safety policy that can be downloaded here.

At Home

The internet is already part of many children's daily life at home – they use it to learn, play, socialise and express themselves. It's a highly creative place of amazing opportunities and an excellent learning tool. However, the technology children use every day can seem complicated at times and you may worry about the risks your child can face online – such as cyber-bullying, contact from strangers or the possibility of them encountering illegal or inappropriate content.

Creating a comfortable environment and creating a place for dialogue to discuss any of these issues is a great starting point; a child knowing they can approach you about these issues is more likely to speak out about them. To support you with this here are a few things you can do:

- Ask your children to tell you about the sites they like to visit and what they enjoy doing online.
- Ask them about how they stay safe online. What tips do they have for you, and where did they learn them? What is OK and not OK to share?
- Ask them if they know where to go for help, where to find the safety advice, privacy settings and how to report or block on the devices and apps/games that they use.

- Encourage them to help. Perhaps they can show you how to do something better online or they might have a friend who would benefit from their help and support.
- Think about how you use the internet as a family. What could you do to get more out of the internet together and further enjoy your lives online?

Parent Resources:

There are a wide range of organisations that offer support for parents in helping keep their children safe online. Below is a selection of recommendations:

NSPCC NetAware (https://www.net-aware.org.uk/)

Safer Internet Centre (https://www.saferinternet.org.uk/)

Childnet (https://www.childnet.com/)

Internet Matters (https://www.internetmatters.org/)

The National Crime Agency have a dedicated child protection department, CEOP. They offer a range of resources for staying safe online and a direct means of reporting inappropriate communications.

CEOP Police (https://www.ceop.police.uk/safety-centre/)

The Department of Education also offers advice and support for parents.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. They will be supported in this by the lead practitioner for IT and Computing.

It is the role of the IT and Computing lead to keep abreast of current issues and guidance through organisations such as CEOP and 'Think U Know'. The lead practitioner updates Senior Management Team when appropriate.

All Governors have an understanding of the issues at our school in relation to local and national guidelines and advice. Writing and reviewing the e-Safety policy (for staff, governors, visitors and pupils), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: ICT, Home-school agreements, Behaviour, Health and Safety, Child Protection, and PSHE policies including Anti-bullying. Our e-Safety policy has been agreed by the Senior Management Team and Staff. The eSafety policy and its implementation are reviewed annually.

E-Safety skills development for staff

- All members of staff receive regular information and training on e-Safety issues through the lead practitioner at staff meetings.
- All members of staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All new members of staff receive information on the school's Acceptable Use Agreement as part of their induction.
- External organisations using the school's ICT facilities must adhere to the e-Safety policy.

Using the internet at school

- The school will provide opportunities within a range of curriculum areas to teach 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 eSafety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when

using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.

- The school Internet access will be designed expressly for pupil use and all devices that allow children internet access will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Managing Internet Access Information system security

- School ICT systems capacity and security will be reviewed regularly.
- System security is overseen by our network managers (ION) and ISP (RM).

Published content and the school website

- The contact details on the school website are the school address, e-mail and telephone number. Staff or pupils' personal information is not published. Material on the school website is monitored by the lead practitioner for IT and Computing. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Written permission from parents or carers will be obtained before photographs or videos of pupils are published on the school Website. 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 permission, in writing, at any time.
- Pupils' full names will not be used anywhere on the school website, particularly in association with photographs.
- Pupils' work can only be published by outside agencies with the permission of the pupil and parents.
- Photographs or videos taken by parents/carers for personal use. In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, social media or for commercial purposes.
- The school blocks access to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate and or illegal (e.g. Facebook) for primary aged pupils.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- School staff are strongly advised not to add children, or parents as 'friends' if they use these sites.

Digital Media, Devices and Streaming

- The use of portable media such as memory sticks, external hard-drives and CD/DVD ROMS will be monitored closely as potential sources of computer virus and inappropriate material. School staff are made aware that they are accountable for the content of any digital media they introduce to the school system.
- Pupils are not allowed to bring personal mobile devices/phones to school without prior agreement from their class teacher. Any phones that are brought to school are sent to the school office and kept there until the end of the day.

- Staff may access external websites that host streaming video or other digital content for the purposes of education. Staff are made aware that they are responsible for previewing and assessing the appropriateness any content they choose to stream.
- Staff are permitted to disable the school's filtering system on their devices to access educational content that they have assessed as safe. This does not apply to devices used by pupils, which must use the school's filtering system at all times.

Remote learning and Google Classroom

- Parents and staff should refer to the school's Remote Learning Policy to ensure pupils and staff remain safe when remote learning is taking place.
- The school uses Google Classroom and PurpleMash to provide remote access to education.
- Teaching staff are responsible for monitoring the content posted in their classroom and the online communications of pupils within their classroom space. Any concerns should be immediately reported to a member of the Senior Leadership Team or dealt with in accordance with the school's child protection policy, if applicable.
- Pupils and parents will be given specific guidance with regard to good conduct when using the school's remote learning platforms.

Protecting personal data

- The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school/West Berkshire Council.
- The school will hold personal information on its systems for as long as individual members of staff remain at the school and remove it in the event of staff leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with applicable data protection legislation. Each teacher has the right to view personal information that the school holds and to have any inaccuracies corrected.

Managing Internet Access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use of IT Agreement for pupils and abide by the school's e-Safety guidelines.
- Access to the Internet will be by directly supervised and to specific, approved on-line materials.
- All staff using a school laptop will be made aware of the schools Acceptable Use of IT Policy
- Adult users are provided with an individual network username and password and email account (RM Unify). Teaching staff will have access to Google Classroom, their user being linked to their RM Unify account.
- All members of staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, email and Google Classroom.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. The IT and Computing lead practitioner will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.

Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the IT and Computing lead practitioner.
- Deliberate access to inappropriate materials by any user will be dealt with in accordance with the school child protection procedure.

- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the Complaints procedure accessible on the school website.

Reviewed: Spring 2021

Next review: Spring 2024