The Redstart Learning Partnership

E-Safety Policy

Buckland St. Mary Church of England Primary School

Castle Primary School

Template Agreed by

The Education Committee of TRLP Board of Trustees: 09/02/23

Review Date: 09/02/25

SIGNED: **DATE: 14/02/23**

Chair of the TRLP Board

Introduction

In The Redstart Learning Partnership (TRLP) believe that computing is central to all aspects of learning; for adults and children in both the school and the wider community. Provision should reflect the rapid developments in technology. We acknowledge **"Children are taught about how to keep themselves and others safe, including on-line……..effective education will be tailored to the specific needs and vulnerabilities of individual children….." KCSiE 2022 (129)**

Computing in the 21st Century is 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, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

All children, whatever their needs, will have access to a range of up to data technologies. Computing is a life skill and should not be taught in isolation.

Computing 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 internet technologies children are using both inside and outside of the classroom include but not wholly:

- Websites
- Learning platforms and virtual learning environments
- Email and instant messaging
- Gaming
- Mobile/smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

All users need to be aware of the range of risks associated with the use of these internet technologies.

Within TRLP, 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, in and beyond the context of the classroom.

'Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach… Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks' (Becta Safeguarding Children Online Feb 2009)

This e-safety policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communication as a whole.

Whole school approach

All members of the school community have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.

The ICT leaders will ensure they are up to date with current guidance and issues through organisations such as ELIM, Becta, CEOP (Child Exploitation and Online Protection), LGFL advice and Child Net.

They then ensure that the Head of School (HoS); senior team and trustees are updated as necessary.

All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website
- procedures in the event of misuse of technology by any member of the school community
- their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff and students receive information on the TRLP's ICT User Policy as part of their induction. Supply teachers must sign to say they have read the ICT User policy before using technology equipment in school.

E-safety in the curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety.

We provide opportunities within the Computing and PSHE curriculum areas to teach about e-safety.

Educating pupils on the dangers of technologies that may be encountered outside school is done as part of the curriculum and informally when opportunities arise.

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 are taught 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 (cyber bullying)

Pupils are taught to critically evaluate materials and learn good searching skills through cross-curricular teacher models, discussions and via the ICT curriculum

Pupils are taught about the risks inherent in using social media, particularly if people they do not know contact them

Managing Internet Access

Children will have supervised access to internet resources

Staff must preview any recommended sites before use. Particular care must be taken when using search engines with the children as these can return undesirable links.

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 recheck these sites and supervise this work. Parents need to be advised to supervise any further research.

Our internet access is controlled through a filtering service provided by either RM or Smoothwall.

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 an ICT leader, technician or member of SLT.

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.

E-mail

The use of email within school is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school, between schools or international. We recognise that pupils need to understand how to style an email in relation to their age.

Pupils are introduced to email as part of the Computer Science Scheme of Work.

The Trust gives staff their own email account, to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

Under no circumstances should staff contact pupils or parents using their personal email addresses.

Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

The forwarding of chain letters is not permitted in school.

Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.

All pupils must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.

Staff must inform a member of SLT if they receive an offensive e-mail.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:

- on the school web site
- on remote parental communication platforms used by the school such as Dojo/Seesaw/ tapestry
- in display material that may be used in external areas, e.g. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

Pupils' names will not be published alongside their image and vice versa without permission from the parents. Full names will not be published.

Social networking and personal publishing

We block/filter access for pupils to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils

Pupils will be advised never to give out personal details of any kind, which may identify them or their location.

Managing emerging technologies

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

Mobile phones will not be used during lessons or formal school time. Their use by children is discouraged but if after consultation with the parents it is felt that there is a need. The phone will be handed in on arrival and collected on departure. The sending of abusive or inappropriate text messages is forbidden.

School photography, assessment notes, emails, music and educational applications will always be done on school equipment and not personal devices.

Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018

Data can only be accessed and used on school computers. 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. The school cannot accept liability for material accessed, or any consequences of internet access. Complaints relating to e-safety should be made to a member of the senior leadership team. Any complaint about staff misuse must be referred to the Head of School.

All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.

For Staff: Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Head of School/ TRLP, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

For Pupils: Deliberate access to inappropriate materials by any user will lead to the incident being logged and dealt with using the Trust behaviour policy.

Pupils and parents will be informed of the procedure.

Parents and pupils will need to work in partnership with staff to resolve issues.

Cyberbullying

Cyberbullying is the use of computing, particularly mobile phones and the internet, to deliberately 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, these are listed in Appendix 2.

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our e-safety curriculum.

Additional online advice on how to react to Cyberbullying can be found on

www.kidscape.org and www.wiredsafety.org

All cyber bullying incidents should be recorded and investigated in the incident log as any other bullying incident. We will then investigate fully as any other bullying incident (refer to behaviour policy)

Working in Partnership with Parents

Parents/carers are asked to read through and sign acceptable use of ICT agreements on behalf of their child on admission to school (see appendix 1).

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 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.

Reviewing this Policy

There will be an on-going opportunity for staff to discuss with SLT any issue of safety that concerns them.

This policy will be reviewed every 24 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Appendix 1

ICT Acceptable Use Policy – Parental Agreement

Dear Parent/ Carer,

The use of Computing including the Internet, e-mail, learning platforms and today's mobile technologies are an integral element of learning in our school. In making this as successful and as beneficial as possible for all learners, we expect all pupils to act safely and responsibly when using technology both within, and outside of, the school environment. We review our E-Safety policy annually and have just updated our Acceptable Use Policy.

The enclosed ICT Acceptable Use Policy forms part of the wider School E-Safety Policy and in association with both the school's Behaviour Management Policy and Home-School Agreement, outlines those principles we expect our pupils to uphold for the benefit of both themselves and the wider school community. I would therefore ask that you please read and discuss the enclosed eSafety Acceptable Use Policy with your child and return the completed slip at the bottom of this page as soon as possible.

If you would like to find out more about eSafety for parents and carers, please visit the ThinkUKnow website at: www.thinkuknow.co.uk. There is a range of parental control software available online (either free or for purchase) which you may like to consider if you have not got this already.

If you have any concerns or would like to discuss any aspect of eSafety, please contact the school office for further guidance.

Kind regards

S Morton

ICT Acceptable Use Policy for pupils:

Agreement / E-Safety Rules

I will take care when using the school IT equipment and use it properly

I will only share my username and password with trusted adults

I will tell an adult if I see anything that upsets me

I will make sure that when I blog I am responsible, polite and sensible

I will use a safe name and not my real name on the internet

I know I am only allowed to go on the internet if my teacher has given me permission

I will only take a photograph or video of someone if they say it is alright

Any messages I send will be polite

I will not deliberately write anything, which upsets other people

I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment

I understand that if I do not follow these rules I may not be allowed to use the school computer or internet for a while, even if it was done outside school

Parent/ Carer signature

We have discussed this and …… (child's name)

agrees to follow the E-Safety rules and to support the safe use of computing as part of The Redstart Learning Partnership.

Parent / Carer Name (PRINT) ……

Parent / Carer (Signature) ……

Class …… Date……

Appendix 2 – Common types of cyber bullying

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 chatrooms.

Instant messaging (IM) — unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger) or Yahoo Chat.

Bullying via websites and social networking sites — use of defamatory blogs, personal websites and online personal "own web space" sites.

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.