PYRFORD CHURCH OF ENGLAND PRIMARY SCHOOL

E-SAFETY POLICY

Approval Date: Autumn 2023

Review Date: Autumn 2024

With reference to the following legislation and statutory guidance:
The Education and Inspections Act 2006
The Education Act 2011
Keeping Children Safe in Education (KCSIE) guidance 2023

Pyrford Church of England Primary School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment

E-safety is part of the school's safeguarding responsibilities, and as such, the Designated Safeguarding Lead (DSL) has lead responsibility for online safety. This policy relates to other policies including those for relationships education, electronic devices, data protection, social media, behaviour, safeguarding, anti-bullying, data protection and using images of children.

Using this policy

- The school has an e-safety coordinator – Lizzie Wright.
- The e-safety policy and its implementation will be reviewed annually. The governing body has overall responsibility for monitoring the policy and holding the headteacher to account for its implementation.
- The e-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and handheld games consoles used on the school site.
- The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff/pupil.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside the school.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform e-safety policy.
- The security of school IT systems will be reviewed regularly.

- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Internet use

The school will provide an age- and needs-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

All communication between staff and pupils or families will take place using school equipment and/or school accounts, including Seesaw and ScoPay.

Pupils will be advised not to give out personal details or information which may identify them or their location.

All videos and images shared with pupils and parents are closely monitored. Videos from You Tube and other sites are shared through the Viewpure filtering website to ensure that only the intended video is viewed.

Email

- Staff may only use approved email accounts on the school IT systems.
- Staff to parent email communication must only take place via a school email address or from within the learning platform.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.

Published content, eg school website, school social media accounts

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing and sharing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school website or any social media.
- Parents are informed that videos and images posted on Seesaw are not to be downloaded or shared.

Use of social media

- The school has a separate Social Media policy.

National Support School
designated by

National College for
Teaching & Leadership

Ofsted
Outstanding
School
2012|2013

- The pupils do not have access to social networking sites in school.
- Staff should ensure that their online activity, both in school and out, takes into account the feelings and privacy of others and is appropriate for their situation as a member of the school community.
- Pupils are taught the risks of social media use and their digital footprint as part of the E-Safety curriculum.

Use of personal devices

- See Personal Electronic Devices policy.

Protecting personal data

- The school has a separate Data Protection Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, and remote access to school systems.

Policy Decisions

Authorising access
- All staff receive information on Acceptable Use / ICT Code of Conduct in the Employee Handbook before accessing the school IT systems.
- At EYFS & Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved online material.
- At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.

Assessing risks
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints and concerns
- Complaints or concerns of internet misuse, including cyber-bullying, will be dealt with according to the school behaviour policy.
- Complaints or concerns of a child protection nature must be dealt with in accordance with safeguarding / child protection procedures, set out in the Child Protection & Safeguarding Policy.

- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school's behaviour policy.

Communication of the Policy

To pupils

- Teaching E-safety is a part of the whole school computing / PSHE / RSE curriculum.

To staff

- All staff will be shown where to access the e-safety policy and its importance explained.
- All staff receive a copy of the Employee handbook which details use of the school IT systems and use of internet whilst on school premises.
- All staff will receive e-safety training as part of the safeguarding training.

To parents

- The school will ask all new parents to sign the Acceptable Use Policy as part of the Admissions Form when they register their child with the school.
- Parents' and carers' attention will be drawn to the school e-safety policy in newsletters and on the school website.
- Parents and carers are given updates on e-safety issues, when necessary, via the school newsletter, email and Seesaw.

Appendix 1

E-Safety Rules

Key Stage 1

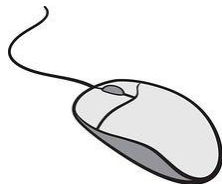# Acceptable use of the school computers

These rules help me to stay safe on the internet

I will take care of the school computers

I will only use the internet when I have been given permission by an adult

I will tell an adult if I see something on the internet that upsets me

I will not tell other people personal things about me

I will always be polite and friendly when I write messages on the internet

THE NEWARK TRUST

Key Stage 2

Acceptable use of the school computers

These rules will help to keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework

- I will not tell anyone my login and password

- I will only login to the school systems as myself

- I will only edit or delete my own files

- I am aware that some websites and social networks have age restrictions which mean that I should not go on them

- I will only visit internet sites that are appropriate for my age

- I will only communicate with people I know, or that a responsible adult has approved

- I will only send polite and friendly messages

- I will not open an attachment, or download a file, unless I have been given permission by an adult

- I will not tell anyone my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission

- If I see anything I am unhappy with or I receive a message I do not like, I will show a responsible adult

My name: …………………………………………….   Date: ……………………….

THE NEWARK TRUST

Appendix 2
SMART poster for children

be SMART!

SAFE- Keep safe by being careful not to give out personal information- such as your real name, school, email address, phone number and password.

MEETING- Meeting someone you have only been in touch with online can be very dangerous! Only do so when a parent or carer is present. Remember online friends are still strangers even if you have been talking to them for a long time.

ACCEPTING- Accepting emails, IM or DM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

RELIABLE- Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or someone who knows. Only chat to your real world friends and family.

TELL- **Tell your parent, carer, teacher or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied or is worried about something online.**

THE NEWARK TRUST

Appendix 3
Information & Tips for Parents

Keeping Our Children Internet Safe At Home

The internet can be a very useful and fun place for our children but we also need them to understand that it can also be a very dangerous place where they can all be vulnerable to bullying, abuse and open to images and information which is not suitable, if not illegal. It is important that we help our children keep the internet a safe and enjoyable place for themselves.

You can teach your children the SMART rules:

SAFE- Keep safe by being careful not to give out personal information- such as your real name, school, email address, phone number and password.

MEETING- Meeting someone you have only been in touch with online can be very dangerous! Only do so when a parent or carer is present. Remember online friends are still strangers even if you have been talking to them for a long time.

ACCEPTING- Accepting emails, IM or DM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

RELIABLE- Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or someone who knows. Only chat to your real world friends and family.

TELL- **Tell your parent, carer, teacher or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied or is worried about something online.**

Top Tip! Only allow internet use in areas at home where you can be aware of what your child is doing. A no internet rule in bedrooms is a good idea.

Useful website- www.thinkuknow.co.uk

We hope that you have found this information useful. If you do have any concerns please feel free to speak to your child's teacher or another member of our staff.