NON STATUTORY

Acceptable Use of ICT policy (Replacing e-Safety)

Purley CE Primary School

Date of policy: December 2020

Review Cycle: Annual

Reviewed By: Full Governing Body

Approved By: Full Governing Board 7th December 2023

Last Reviewed: Autumn 2023

Next review date: Autumn 2024

Learn to love, love to learn

'Let all that you do be done with love', 1 Corinthians 16:14

Change History

Version	Date	Description	Change ID
1.0	Autumn 2020	Final Version of Acceptable use of ICT policy (replacing e-Safety Policy)	Clerk
2.0	Autumn 2021	Annual update	Clerk
3.0	Autumn 2023	Annual update	HG

Contents

1. Aims

- To have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community and its use of technology.
- Establish clear mechanism to identify, intervene and escalate an incident, where appropriate.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
The policy also takes into account the National Curriculum computing programmes of study

3. Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

All governors will agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

All staff and volunteers
All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet.

Parents
Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: parents-factsheet-11-16.pdf (childnet.com)

Visitors and members of the community
Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, and expected to follow it.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

The text in italic below is taken from the National Curriculum computing programmes of study.

*In **Key Stage 1**, pupils will be taught to:*

Use technology safely and respectfully, keeping personal information private;

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Early years and KS1 will be taught to:

- Only use the internet when an adult is present.
- Keep personal information and passwords safe and understand its importance.
- Only send messages that are polite and friendly.
- Be aware that the school can monitor activity.
- Sanctions e.g. limiting access if rules are not followed.
- Tell an adult/teacher if something online causes unhappiness or worry.

*Pupils in **Key Stage 2** will be taught to:*

Use technology safely, respectfully and responsibly;

Recognise acceptable and unacceptable behaviour;

Identify a range of ways to report concerns about content and contact.

Pupil in Key Stage 2 (age 7-11 years) will be taught:

Safe

- Only send polite and friendly messages.
- Only post appropriate pictures or videos.
- Only talk with and open messages from known people.
- Be aware that people online may not always be who they say they are.
- Report to a teacher if anyone is being unsafe with technology.
- Talk with an adult if unsure about something, or if something happens online which causes worry or fright.
- Minimise page if seeing anything that causes upset or worry and tell an adult straight away.
- Keep personal information and passwords safe and private and understand its importance.

Trust

- Be aware that not everything online is honest or truthful.
- Always credit the person or source that created any work.

Responsible

- Only use websites and search engines that the teacher has sanctioned.
- Only use school computers and school email identity/email address (or any other technology) for school work unless permission has been given otherwise.
- Personal devices e.g. mobile phones are not permitted to be used during the school day without permission. They must be turned off and handed to the teacher at the start of the day and collected at the end of the school day.
- Only change settings with permission.
- Understand that the school's internet filter is there for protection.
- Know that the use of school devices and internet access will be monitored.
- Know that irresponsible use will result in withdrawal of access.
- Being responsible means not looking for bad language, inappropriate images or unsuitable games.
- Do not pretend to be anyone else.
- Do not access or change other people's files, accounts.
- Know that online actions have offline consequences.

E-safety

- E-safety posters will be posted around the school.
- The children receive e-safety lessons and are constantly reminded of online safety.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Pupils should only invite known friends and deny access to others.
- The safe use of social media and the internet will be covered throughout the curriculum.
- The school will use school assemblies and parent newsletters to raise awareness of dangers.

Social networking and personal publishing
The school will deny access to social networking sites and pupils will be advised not to use these at home.

5. Acceptable use of IT

As a professional organisation with responsibility for safeguarding, it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner.

Staff must understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices e.g. laptops, mobile phones, tablets, digital cameras, email and social media sites.

The Computer Misuse Act 1990 makes the following, criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

Users will need to:

- Understand that any hardware and software provided by Purley School for staff use can only be used for educational purposes.
- To prevent unauthorised access to systems or personal data, do not leave any information system unattended without first logging out.
- Respect system security and not disclose any password or security information. Use a 'strong' password to access school systems.
- Do not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- Ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection legislation (including GDPR).

- Any data being removed from the school site (such as via email or on memory sticks or CDs) will be suitably protected.

- Respect copyright and intellectual property rights.
- Immediately report any illegal, inappropriate or harmful material or incidents to the Designated Safeguarding Lead /Headteacher.
- Do not attempt to bypass any filtering and/or security systems put in place by the school.
- Report to the Headteacher any suspicion that a computer or system has been damaged or affected by a virus or other malware.
- Report any loss of any school related documents or file to the Headteacher.
- Electronic communications with current or past pupils, parents/carers and other professionals will take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
- Communication will take place via school approved communication channels, such as a school provided email address or telephone number, and not via personal devices or communication channels, such as personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Headteacher.
- Ensure that personal online reputation and use of IT and information systems are compatible with a professional role, whether using school or personal systems.
- Take appropriate steps to protect one's self online and ensure that use of IT and the internet will not undermine professionalism, interfere with work duties and will be in accordance with the school code of conduct/behaviour policy and the Law.
- Do not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or cause needless anxiety to any other person, or anything which could bring the profession, the school, or the County Council, into disrepute.
- Understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance. Where it believes unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.
- All staff will have access to this policy and its importance explained.
- The use of the school's name, logo, or any other published material should not be used without written prior permission from the Headteacher.
- All staff will receive refresher training as part of safeguarding training.
- All new staff members will receive training as part of their induction.

Social Networking

- Staff are **strongly advised** not to add pupils as 'friends' into their personal accounts (including past pupils under the age of 18).
- Staff are **advised** not to add parents as 'friends' into their personal accounts.
- Staff **must not** post comments about the school, pupils, parents or colleagues including members of the Governing Body.
- Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards.

- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'.
- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.
- It is recommended that management and school staff do not identify their school on social networking sites as this could directly link their behaviour outside of work with the reputation of the school.

Cameras (including iPads etc)

- Photographs taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements is an effective form or recording their progression. However, it is essential that photographs are taken and stored appropriately to safeguard the children in our care.
- Wherever possible, only the designated school cameras and iPads are to be used to take any photo within the school or on outings. Images taken must be deemed suitable without putting the child/children in any compromising positions that could cause embarrassment or distress.
- If personal devices are used, photos must be deleted immediately after uploading to school storage and Headteacher informed.

Mobile Phones

- Pupils may bring mobile devices into school, but are not permitted to use them during lessons, clubs before or after school, or any other activities organised by the school
- The school allows staff to bring in personal mobile telephones and devices for their own use.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- All staff must ensure that their mobile telephones/devices are left inside their bag throughout contact time with children.
- Mobile phone calls may only be taken at staff breaks or in staff members' own time.
- If staff have a personal emergency they are free to use the school's phone or make a personal call from their mobile away from children.
- Staff (will need to) ensure that the school has up to date contact information and that staff make their families, children's schools etc. aware of emergency work telephone numbers. This is the responsibility of the individual staff member.
- It is the responsibility of all members of staff to be vigilant and report any concerns to the Headteacher.
- Concerns will be taken seriously, logged and investigated.
- The Headteacher reserves the right to check the image contents of a member of staff's mobile phone should there be any cause for concern over the appropriate use of it.

Parents/carers

- Parents and carers will be made aware of their responsibilities regarding their use of social networking.
- Methods of school communication include the prospectus, the website, newsletters, letters, parent mail, social networking sites and verbal discussion.
- School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion.
- Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.
- Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event without parental permission.
- Parents should make complaints through official school channels rather than posting them on social networking sites.
- Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

6. Handling e-safety complaints

- Staff will deal with complaints of pupil internet misuse and escalate to Headteacher if deemed more extreme.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with the school's Child Protection Procedures.

Dealing with incidents of online bullying/inappropriate use of social networking sites

- The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.
- In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy, and will send a letter.
- The Governing Body understands that, "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written…which:
    - expose (*an individual*) to hatred, ridicule or contempt
    - cause (*an individual*) to be shunned or avoided
    - lower (*an individual's*) standing in the estimation of right-thinking members of society
    - Disparage (*an individual*) in their business, trade, office or profession. (National Association of Headteachers)
- Records should be kept of the abuse, text, e mails, website or instant messaging and carefully record the time, date and place of the site.

7. Monitoring arrangements

Due to the ever-changing nature of information and communication technologies, this policy is to be monitored and reviewed annually by the Governing Body.

8. Links with other policies

This policy was written with reference to a range of guidance with consideration of the school's church school ethos.

This policy should be considered alongside other related policies in the school:

- Safeguarding Policy
- Whistleblowing Policy
- Safer Recruitment Policy
- Behaviour in schools [inc. Anti-bullying]
- Health and Safety Policy.