

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:

Last Reviewed: Autumn 2025

Next review date: Autumn 2026

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
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
4.0	Autumn 2024	Changes made in line with KCSIE 2024 and using model Policy from The Key	AH
5.0	Autumn 2025	References to KCSIE updated in line with Sept 2025 publication	AH

Contents

1. Aims
2. Legislation and guidance
3. Definitions
4. Roles and responsibilities
5. Unacceptable Use and Sanctions
6. Educating pupils about online safety
7. Access to school ICT facilities and materials by Staff
8. Access to school ICT facilities and materials by Pupils
9. Monitoring and Review
10. Links with other policies

Appendix

Social Media information sheet for staff

Aims

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors. Breaches of this policy may be dealt with under our school's behaviour policy or staff code of conduct.

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 and the recommendations set out in Keeping Children Safe In Education 2024.

3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user

- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

4. 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: <https://www.childnet.com/resources/parents-and-carers-resource-sheet/>

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.

5. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour and the staff code of conduct.

6. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum. We follow the Purple Mash Scheme of Work. We also take on board their recommendation that "... online safety is not only taught discretely through computing but additionally during PSHE lessons and whole school sessions and as part of other subjects where pupils might use technology, such as for email, blogging and online research."

The text in italics 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 **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.*

All pupils will be taught the below acronym:



[Source: 2 Simple/Purple Mash]

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.

7. Access to school ICT facilities and materials by Staff

The school's ICT Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Manager.

7.1 Use of phones and email

The school provides each member of staff with an email address:

- This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s).
- All work-related business should be conducted using the email address the school has provided.
- Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error that contains the personal information of another person, they must inform the Headteacher.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Recording phone conversations

The school can record incoming and outgoing phone conversations. All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

If you record calls, callers must be made aware that the conversation is being recorded and the reasons for doing so.

Explain when you record phone conversations and why. For instance:

"Calls are recorded for use in staff training"

Staff who would like to record a phone conversation should speak to the Headteacher

They may grant requests to record conversations when:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions

- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays or reasons for absence

7.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The headteacher may withdraw or restrict this permission at any time and at their discretion. Personal use is permitted provided that such use:

- Does not take place during teaching hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken. Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media (see appendix 1) and use of email to protect themselves online and avoid compromising their professional integrity.

7.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

8. Access to school ICT facilities and materials by Pupils

Handling e-safety complaints

- Staff will deal with complaints of pupil internet misuse, logging these on our CPOMS Safeguarding tool
- 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.

9. Monitoring and Review

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

10. 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 Policy
- Anti Bullying Policy
- Health and Safety Policy
- Staff Code of Conduct

Appendix 1: Social Media information sheet for staff

Do not accept friend requests from pupils on social media

10 rules for 'best practice' by school staff on Social Media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the social media app from your phone. The apps can recognise WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to '**Friends only**', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've '**liked**', even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public

- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if ...

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
 - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
 - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police