Curwen Primary School

Together Everyone Achieves More

COMPUTING POLICY

Date of review: Summer 2025 **Date of next review: Summer 2028**

1. Teaching and Learning

1.1 Curriculum

Using the Curwen Computing Scheme, year groups follow a yearly overview ensuring coverage and progression of all units and skills and knowledge. The National Curriculum objectives are included and are in bold throughout the scheme. Lessons are taught as a mixture of learning discreet Computing skills, and how to apply these to different situations. Where possible, this is coherently linked with other curriculum areas ensuring meaningful links are made, and pupils can see tangible outcomes of the application of skills and knowledge.

1.2 Cross Curricular Use of Computing

Computers are a powerful tool which can be used to enhance teaching and learning across the curriculum, challenging the most able while supporting those children who find the technology difficult to use. Pupils will be taught and given opportunities to consolidate skills through highly motivating cross-curricular activities.

This will be achieved as follows:

- Meaningful links made to Computing skills across curriculum areas enabling pupils to use their skills and knowledge for purposeful activities.
- When planning lessons involving the use of Computing, teachers ensure key skills are taught and pupils are expected to apply to a variety of situations.
- Pupils are given the skills to enable them to choose appropriate systems and programs relevant to the task they are completing.
- Homework is now completed using Google Classroom from Year 1-6, ensuring appropriate skills are consolidated in real life situations, bringing their skills and knowledge learnt in school into this.

1.3 Resources

Curwen Primary School has developed a bank of systems, materials and resources to facilitate the teaching of Computing and will continue to do this. Many of these resources can be booked through the school's ICT Learning and Resources Manager.

These include:

- Each class throughout the school has a trolley of 15 Chromebooks which can be accessed at any time, with the use of 30 in Computing lessons with year groups sharing.
- Each class has a HD LCD interactive whiteboard, and visualiser.
- There is at least one class-based computer in each room.
- There are 3 trolleys of IPads – EYFS, KS1 and KS2
- Programmable toys (Beebots) and assorted mats/roads.
- A range of multimedia sets are available for class use to support learning (including digital cameras, Easyspeaks).

- Packages specifically designed to help children with special educational needs and the use of Apps on the iPad such as Stop Animation.
- The use of Google Classroom to store material, assignments and other important documents for children, so that is in an organised specific place.
- A bank of P.C.-based software to support and supplement the Scheme of Work and promote cross-curricular links.
- Online access to the coding curriculum, which is based around Scratch from Year 1 to Year 6.
- Laptops used by specific staff to develop personal and professional I.C.T. skills but also to facilitate work from home.
- Access to the Computing Lead and Technical Staff full time for network support and hardware management.
- Access to the Computing Lead to support within PPA and lessons.

2. Internet Usage

2.1 Acceptable Use Policy for the Internet

As part of our commitment to the London Grid for Learning we have multi point access to the internet through our Network system. The internet represents an exciting area for children and teachers alike to expand their ability to locate and learn new information. It provides the opportunity for pupils to develop their independence within learning, and communicate on a global level. Through the LGFL and Google staff can deliver electronic communications anywhere in the world – refer to the TTLT Acceptable Use Policy.

2.2 Online Safety

We recognise the importance of the opportunity for all pupils to have access to the internet, but at the same time exercise sensible caution over its implications. As a result, we have introduced guidelines, and have interwoven taught online safety content into our curriculum overviews. This aims to both prevent pupils and staff from accessing inappropriate materials, and to develop an understanding of safe and appropriate internet usage. This is designed to be progressive at age-appropriate levels, and to provide pupils with life skills as they move onto the next stage in their development. Additionally, we constantly update our curriculum

Our separate Online Safety Policy provides full information on school procedures and can be viewed within this.

3. Staff Usage

As part of continuing professional development, we welcome and encourage staff use of the internet. Access is provided by Usernames and Passwords appropriate to Teaching Staff, Teaching Assistants and Administration personnel. As with pupil access, the filtering system operates and staff are protected from unauthorised access.

Staff internet guidelines are as follows:

- Internet searches within school hours are to be based upon curricular research or class-based topic work. Internet searches out of school hours may be focussed upon personal and professional use. Staff should however exercise professional discretion when starting searches on the World Wide Web.
- Staff may use e-mail at any time before and after school but should be aware that they are using a school facility and their communications should not contain anything which could cause offence.

- Staff may use the school e-mail system or their own e-mail accounts for personal use, but must be aware of the need to exercise professional discretion when sending and receiving e-mail.

4. Links with other policies

This policy links to the following policies and procedures:

- EYFS Policy
- Assessment Policy
- Marking and Feedback Policy
- SEN policy and information report
- Equality information and objectives
- Individual subject policies
- Curriculum Statement
- Pupil Premium Strategy
- Curriculum Policy
- TTLT Acceptable Use Policy

C P S

Curwen Primary School

Together Everyone Achieves More

The Tapscott Learning Trust
Working together, achieving for all

ONLINE SAFETY POLICY

Date of review: Summer 2025 **Date of next review: Summer 2028**

This document should be read in line with the Computing Policy and the Staff Code of Conduct which includes use of technology.

1. Rationale

1.1 The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Curwen Primary School with respect to the use of ICT-based technologies
- Safeguard and protect the children and staff of Curwen Primary School
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use
- Have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Minimise the risk of misplaced or malicious allegations made against adults who work with students

2. The main areas of risk for our school community can be summarised as follows:

2.1 Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

2.2 Contact

- Grooming
- Online bullying in all forms
- Terrorism and extremist material
- Identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords

2.3 Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (Internet or gaming))
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)

2.4 Commercialism

- copyright (little care or consideration for intellectual property and ownership – such as music and film)
- Phishing and Scamming emails and messages
- Cookies and use of ads
- Micro-transactions in play stores and within previously owned apps

3. Education and Curriculum

3.1 Pupil online safety curriculum

Curwen has a clear, progressive online safety education programme as part of the Computing curriculum / PSHE curriculum. The overview for this programme is outlined in our Computing and PSHE curriculum. It is built on LA / LGfL e-safeguarding and e-literacy framework for EYFS to Y6. Furthermore, through pupil surveys and staff meeting, we have included several things that are appropriate for Curwen, based on current or past incidences in the school.

The programme covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
- To know how to narrow down or refine a search
- [For older pupils] To understand how search engines work and to understand that this affects the results they see at the top of the listings
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- To understand why they must not post pictures or videos of others without their permission.
- To have strategies for dealing with receipt of inappropriate materials
- [For older pupils] To understand why and how some people will 'groom' young people
- To understand the impact of online bullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
- To know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button
- Plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming / gambling
- The statutory guidance (Prevent Duty) makes clear the need for our school to ensure that children are safe from terrorist and extremist material when accessing the internet in school. We have a Prevent Risk Assessment that staff are familiar with. We provide yearly training for staff to identify and report any issues relating to terrorism/extremism.
- To ensure that suitable filtering is in place

3.2 Staff Training

This school:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
- Makes regular training available to staff on online safety issues and the school's online safety education programme
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy, TTLT Data Protection Policy and Safeguarding Policy
- Provides staff with cyber activity training, which entails developing good habits in anticipating fake emails and general internet search

3.3 Parent awareness and training

This school:

- Runs a rolling programme of advice, guidance and training for parents, including:
  - Information leaflets; in school newsletters; on the school web site
  - Demonstrations, practical sessions held at school
  - Suggestions for safe Internet use at home
  - Provision of information about national support sites for parents
  - Inform parents of latest developments in ICT and technology, and ways of promoting Online Safety through parents' workshops

4. Expected Conduct and Incident Management

4.1 Expected conduct

In this school:

All users

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems (at KS1 it would be expected that parents/carers would sign on behalf of the pupils)
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on online bullying
- Are responsible for ensuring age-appropriate content when using videos from YouTube. This includes children not being exposed to live advertising

Staff

- Are responsible for reading the school's Online Safety Policy / Staff Code of Conduct and using the school ICT systems accordingly, including the use of mobile phones, and hand-held devices
- Understanding and using complex password to protect data
- Are responsible for reporting / logging any inappropriate use that they may be made aware of

Students/Pupils

- Should work towards having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Understanding and using complex password to protect data

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form at time of their child's entry to the school
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse
- Will be informed in the event of any inappropriate use of technology that has been identified within school, and additional support/training offered as relevant

4.2 Incident Management

In this school:

- There is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school. The records are reviewed / audited and reported to the school's senior leaders, LAB members / the LA / LSCB
- Parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

5. Managing the ICT infrastructure

5.1 Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files
- Uses Malwarebytes software which adds extra protection against ransomware, spyware, adware, virtues and other malware (From LGFL)
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network
- Uses security time-outs on Internet access where practicable / useful
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns
- Ensures pupils only publish within an appropriately secure environment: Google Classroom
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required. e.g. kidrex, kiddle or ask for kids , Google Safe Search
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search.
- Informs all users that Internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the [*ICT Learning Resource Manager / teacher / person responsible for URL filtering]*. Our system administrator(s) logs or escalates as appropriate to the technical service provider or LGfL Helpdesk / Turn It On (TIO) as necessary
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents

6. E-mail

This school:

- Provides staff with an email account for their professional use, *London Staffmail / LA email* and makes clear personal email should be through a separate account
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our Internet access to the World Wide Web

7. School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- Uploading of information is restricted to our website authorisers: Key Office Administrators
- The school website complies with the statutory DfE guidelines for publications and the TTLT Freedom of Information Policy
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published
- Photographs published on the web do not have full names attached
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website

8. Learning platform

- Uploading of information on the schools' Learning Platform / Virtual Learning Space / Cloud Storage (Google Drive) is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas
- Photographs and videos uploaded to the schools LEARNING PLATFORM will only be accessible by members of the school community
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform

9. Social networking

Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff

- They do not engage in online discussion on personal matters relating to members of the school community
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

10. Use of AI (Artificial Intelligence)

Teachers and children are able to use AI in line with the TTLT's The Use of AI (Artificial Intelligence) Policy (please refer to TTLT The Use of AI Policy October 2024)

11. CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained on the hard drive for 28 days*), unless deemed to be necessary where disclosed to the Police as part of a criminal investigation

12. Equipment and Digital Content

12.1 Personal mobile phones and mobile devices

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times. These may only be used in the staffroom at break and lunch times
- Mobile phones brought into school are entirely at the staff member, parents' or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff

Students' use of personal devices

- The school strongly advises that student mobile phones should not be brought into school
- The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety
- If a student breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity
- Staff will be issued with a school phone where contact with students, parents or carers is required
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose
- If a member of staff breaches the school policy, then disciplinary action may be taken

- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes
- Refer to Staff Code of Conduct for further information

12.2 Digital images and video

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs / social media materials
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse

13. Monitoring and Reviewing

This policy will be monitored and reviewed to meet the latest information and changes made to keep up with relevant technological updates and statutory requirements. This policy is reviewed every three years.