Rebecca Cheetham Nursery
and Children's Centre

ICT and Online Safety Policy

Author: SLT
Date: April 2024
Ratified by governors:

Governor's signature:_____

ICT Policy

April 2024

This document sets out the Policy for Computing within Rebecca Cheetham Nursery and Children's Centre. It should be read in line with other school policies.

PHILOSOPHY AND AIMS

Philosophy

At Rebecca Cheetham we believe that Information Communication Technology (I.C.T.) and computing are important aspects of education. They help pupils prepare for later life, developing key transferrable skills and understanding of the uses and limitations of I.C.T. As well as being an important curriculum requirement, the ability to use I.C.T. effectively is a vital life skill. At our school and Children's Centre we use I.C.T. as a resource for learning and it is an important tool to raise standards. We offer a mix of different systems within the school to consolidate and extend computer skills and to expand the awareness of technology and its place in the modern world. We recognise that computer and technology skills are crucial if pupils are to raise their achievement and general competence in the use of I.C.T. systems.

Aims

- That we build on each child's previous experience.
- Cultivate the skills that are essential for the children to gain access to developing technologies.
- Promote the children's enjoyment of ICT, building on their experience in everyday life as a basis for learning.
- Evaluate resources and update and add to them as necessary.
- Undertake ICT training and opportunities for all staff.
- To take into account issues relating to inclusion and to allow for differentiation with pupils that need additional help to access learning.
- Be aware of current developments in ICT.
- Use initiative from central and local government, authorities and other bodies to support ICT in the school.
- To ensure the health and safety of pupils, staff and visitors with regard to using ICT (See Ataff acceptable Use of the Internet Policy and Internet Use for Children Policy).
- To develop ICT capability in finding, selecting, and using information.
- To use ICT for effective and appropriate communication.
- To apply the children's ICT skills and knowledge to their learning in other areas of the curriculum.
- To develop children's understanding of everyday uses of information and communications technology.
- To develop technological literacy through a range of products which children will be familiar with and which will be easily understood and accessed.
- To encourage children to work collaboratively, sharing knowledge, skills and enjoyment.
- To develop a skills-based approach to computer use which puts the child in control of the equipment rather than the other way round.
- To encourage children and staff to use the Internet to gain knowledge and support learning.
- To use technology as a means of additional communication with families and the community.

TEACHING AND LEARNING

Curriculum

Using the EYFS Framework as a basis, children are exposed to a variety of ICT and technological equipment to enhance their knowledge and understanding. 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. Children are able to use ICT and other technologies in the child initiated provision as well as during focused learning.

Cross Curricular Use of Information Communication Technology

ICT is 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.

Resources

Rebecca Cheetham Nursery and Children's Centre has an array of different resources to help facilitate the learning of ICT and technology.

These include:

- Staff use iPads / tablets in order to record observations and assessment on the children and the children have access to iPads / tablets as part of the provision (with time limits).
- PCs.
- We offer the children access to Bee-bots (programmable bee robots).
- CD players
- Headphones
- Walkie-talkies
- Torches
- Metal detectors
- Interactive whiteboard (staff and children use the whiteboard)
- We have an ICT technician attending once a week for advice and support.

INTERNET USAGE

Acceptable Use Policy for the Internet

As part of our commitment to the London Grid for Learning we have multi point access to the World Wide Web through our Network system. The school also subscribes to 'Fronter' which provides a safe online learning platform for all staff and pupils known as the 'MLE' (Managed Learning Environment). 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 staff can send electronic communications anywhere in the world.

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 offer parents workshops and information on online safety. This aims to both prevent pupils, staff and outside agencies from accessing inappropriate materials, and to develop an understanding of safe and appropriate internet usage.

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

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, Children Centre staff 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.

ASSESSMENT

Staff use iPads in order to gather evidence for assessing the children. Staff will observe the children using ICT, technology and skills in computing to make assessments against the EYFS framework.

EQUAL OPPORTUNITIES FOR I.C.T.

We believe that all pupils, irrespective of their race, gender, age, class or religion should have equal access to resources. The school will promote equal opportunities for computer usage and fairness of distribution of ICT resources. All members of staff should also have the same rights of access to develop individual skills and promote effective learning.

HEALTH AND SAFETY GUIDELINES FOR I.C.T.

Health and safety guidelines are as follows:

- When locating a computer in a classroom, ensure there are no trailing leads and that no exits are blocked.
- When using laptops, ensure staff collect and return laptops in a safely.
- If any equipment is damaged, cease using and report immediately to the Administration team..
- Ensure staff and pupils do not have food or drinks around laptops or other electrical equipment.
- For further information regarding Health and Safety advice, see the Health and Safety Manager

The Computing Policy will be reviewed by the SLT in line with government requirements.

ONLINE SAFETY POLICY

April 2024

This document should be read in line with the Computing Policy.

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Rebecca Cheetham Nursery and Children's Centre with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Rebecca Cheetham Nursery and Children's Centre.
- 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.
- Ensure staff are compliant in regards to the Data Protection Act and GDPR regulations.

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

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.

Contact

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

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).
- copyright (little care or consideration for intellectual property and ownership – such as music and film) (Ref Ofsted 2013)

2. Education and Curriculum

Online safety

This school:

- Plans 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 sessions.
- Ensures that when copying materials from the web, staff understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.
- Ensures that staff 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. To ensure that suitable filtering is in place.

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.
- 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 and Safeguarding Policy.

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.

3. Expected Conduct and Incident Management

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.
- 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 and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

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.

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, Governors / the LA / LSCB as appropriate.
- 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.

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering and monitoring

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 user.
- 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 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 / School and Children Centre publicity.
- 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.

- Ensures all staff, parents and partners have signed an acceptable use agreement form and understands that they must report any concerns.
- Requires staff to preview websites and video content 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. yahoo for kids or ask for kids , Google Safe Search , …..
- Is vigilant by not conducting 'raw' image search in front of 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 [*system administrator / teacher / person responsible for URL filtering]*. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk 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.

Further filtering and monitoring online activity information

- The governing board ensures the school's ICT network has appropriate filters and monitoring systems in place.
- The headteacher monitors to determine what filtering and monitoring systems are required.
- The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.
- The governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- ICT technicians undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.
- Requests regarding making changes to the filtering system are directed to the headteacher.
- Prior to making any changes to the filtering system, ICT technicians and the DSL conduct a risk assessment.
- Any changes made to the system are recorded by ICT technicians.
- Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.
- Deliberate breaches of the filtering system are reported to the DSL and ICT technicians, who will escalate the matter appropriately.
- If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.
- If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.
- The school's network and school-owned devices are appropriately monitored.
- All users of the network and school-owned devices are informed about how and why they are monitored.
- Concerns identified through monitoring are reported to the DSL who manages the situation.

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.
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- Will contact the Police if one of our staff 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.

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.
- The school web site complies with the statutory DfE guidelines for publications.
- 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.

Google Drive / Cloud Based

- Uploading of information on the schools' 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 Google Drive will only be accessible by members of the school community and with the appropriate permission rights.
- Anything we are saving onto Google Drive is vetted through the Data Protection Policy and Procedures.

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 parents, 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.

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 by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.

5. Equipment and Digital Content

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. Such images are requested not to be shared on social media.
- 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.

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.
- School pool mobile phones should only be used during working hours.
- Ensure that the phone is password protected and if lost or stolen this is reported to a member of SLT immediately.

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.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Parents, through workshops and materials, are advised to be very careful about placing any personal photos on any social media and the need to maintain privacy settings so as not to make public, personal information.
- Parents 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.

Addendum to policy based on COVID – 19 restrictions and remote learning for children

ZOOM calls and access – protocols and safeguarding information – by accessing the zoom call parent/ carers agree to the terms stated below.

- The zoom app needs to be downloaded to a device. This is free to do and there is a download for every type of device: https://zoom.us/download.
- Staff facilitator will use their work account to login to Zoom.
- You will be asked to register your interest by completing a short google form.
- One we have received your form we will then send an email to your email address with the link meeting ID and password, which will allow you to log into the session.
- We ask participants not to share the meeting ID or Password with anyone else.
- Once you have logged in you will be held in the 'waiting room' whereby the lead of the session will admit you into the session.
- When joining the session ensure that your camera is on at all times and your full name is shown rather than a nickname, to enable us to identify you.
- We ask that you mute your microphone unless directed otherwise by the facilitator.
- You are not permitted to take photographs or videos throughout the duration of the session.
- We may require at times to record our session for training purposes, therefore we will inform you prior to this to enable you to make a decision as to whether you would like to participate.
- There will be two practitioners at all times when delivering sessions.
- All those who are participating are asked to wear appropriate clothing when joining.
- Once all are admitted the call will be locked so that no one else can join.
- Positive, appropriate language to be used at all times, including any talk by others in the background.
- When the call is finished the lead practitioner will end the meeting for all