Knowle West Nursery School

We all Matter - We all Belong

Knowle West Nursery School
E-Safety Policy

Date Agreed:	23rd May 2022	**Review Date:**	23rd May 2023
Signed by:	Lesley Edwards	**Signature:**	
Role of Signatory:	Chair of Governors		

1. Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the every day lives of children, young people and adults. Consequently, educational settings need to build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment. Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Knowle West Nursery School (KWNS) we understand the responsibility to educate our children and families in eSafety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. This policy therefore aims to clarify the responsibilities of management and staff when using cameras, mobile phones, computers and games consoles within the setting, to safeguard children's welfare in relation to the above areas and minimize the risk of harm and to fulfil legal duties in relation to personal data and other areas, e.g.: Data Protection Act 1998.

This policy is inclusive of both fixed and mobile internet; technologies provided by the centre; (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc); and technologies owned by families and staff, but brought onto the Centre's premises (such as laptops, mobile phones, camera phones and portable media players, etc).

2. Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the centre, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in our centre is **Jenny McDonald** who has been designated this role as a member of the senior Leadership team. All members of the centre community have been made aware of who holds this post. It is the role of the e-Safety coordinator to keep abreast of current issues and guidance through organisations such Bristol LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

The e-Safety coordinator updates Senior Management and Governors and all governors have an understanding of the issues at our Centre in relation to local and national guidelines and advice.

KWCC Staff should report any concerns about any inappropriate or intrusive photographs found or any activity that raises concerns.

3. Writing and reviewing the e-Safety policy

This policy, supported by the Centre's Acceptable Use Agreement for staff, governors, visitors and children, is to protect the interests and safety of the whole community.

This policy works in conjunction with the following policies: Complaints, Equalities, Health and Safety, Safeguarding, Anti-bullying.

Our e-Safety policy has been written by the Centre, in conjunction with advice from Bristol County Council (BCC), and government guidelines. It has been agreed by the Senior Leadership Team, Staff and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed annually.

4. e-Safety skills development for staff

Centre staff receive regular information and training on e-Safety issues through the coordinator at staff meetings.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the centre community.

New staff receive information on the centre's Acceptable Use Agreement as part of their induction.

All staff are encouraged to incorporate e-Safety activities and awareness within their sessions.

5. E-Safety information for parents/carers

Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.

Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the KWCC website.

The website contains useful information and links to sites like Thinkuknow, Childline, CEOP and the CBBC Web Stay safe page.

The centre will send out relevant e-Safety information through newsletters, the website, and the prospectus.

6. Computer and Laptop

Staff should not use the setting’s computer/laptop for personal use.

The Centre will ensure that all programs used and websites accessed are appropriate and that children are not able to access or download material which is unsuitable.

All setting files that contain personal data will be stored appropriately and securely, e.g.: password protected or locked away.

Staff should not forward any of the settings work, files, information etc stored on the setting computer/laptop to their home PC, unless, this has been agreed by management as necessary practice for the setting. It is recommended that a log of “homework” should be kept in the setting and this needs to be checked and signed by management on a regular basis. Any work taken home needs to be appropriately protected as if it were in the setting and open to scrutiny by management.

Staff should not use any personal memory devices in the setting’s computer/laptop. Memory sticks provided by the setting should be used for work purposes only and should not be taken off the premises.

All ICT equipment should remain in the setting at all times. This is to minimise the risk of computer viruses and for data protection purposes.

Practitioners should not access, copy, remove or otherwise alter any other user’s files, without their expressed permission.

All email communication should be appropriate and written in a professional manner.

Caution should be taken if personal e-mail addresses are used on the setting/laptop.

E-mail attachments should only be opened if they are from a source known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

Illegal or inappropriate materials MUST NOT be uploaded, downloaded or accessed.

Staff should ensure that setting’s computer/laptop is used appropriately to avoid disabling or damaging equipment.

7. Mobile Phone Usage

Mobile phones may be used in settings, as long as their use is appropriate. The use of a mobile phone must not detract from the quality of the supervision and care of children.

Appropriate use is defined as follows:

a. No mobile phones

- Practitioners, volunteers, students etc will not have their private mobile phone on their person during work hours.
- Mobile phones will be kept in a secure area away from where the children are accommodated.
- Staff may use their mobile phones during their designated breaks and in an area away from the children.
- The setting's contact number will be given as an emergency number in case practitioners need to be contacted.
- Setting practitioners are not to use any mobile phone cameras to photograph the children.
- Visitors and parents will be asked to switch off their mobile phones or not to use phones while on the premises. If they need to use their mobile phone they will be asked to do so away from the children.

b. Mobile phones on outings only

- Offsite on outings, mobile phones may be very useful. Where child information is stored on a personal mobile for an outing this needs to be deleted after the outing is over. It is recommended that the senior member of staff records this occurrence. Alternatively paper information may be taken on outings.

c. Mobile phones permitted

- In the setting, use of mobile phones will be for business and emergency purposes and practitioners are not to be distracted from the care of children.
- Setting practitioners must never exchange mobile phone numbers with children in their setting.
- Setting practitioners are not to use any mobile phone cameras to photograph the children, unless, there is a designated setting mobile phone for this purpose.
- Practitioners will be held responsible for the content and security of their own phones, e.g. access to web pages. If this is deemed to be a safeguarding issue this will be dealt with in line with the settings child protection and disciplinary policy.
- Images taken of the setting or its children should be downloaded onto the settings computer/laptop only. Images must not be downloaded onto any personal computer.
- Offsite on outings, mobile phones may be very useful. Where child information is stored on a personal mobile for an outing this needs to be deleted after the outing is over. It is recommended for the senior member of staff to record this occurrence. Alternatively paper information may be taken on outings.

8. Internet

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

The Centre will aim to provide opportunities to teach eSafety to children and families. The Internet access will be designed expressly for child use and will include filtering appropriate to the age of the children.

Educating children on the dangers of technologies that may be encountered outside the setting will be done informally when opportunities arise and as part of the e-Safety curriculum. Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

The Centre will ensure that the use of Internet derived materials by staff and complies with copyright law.

External organisations using the setting's ICT facilities must adhere to the e-Safety policy.

ICT systems capacity and security will be reviewed regularly and virus protection will be updated regularly.

9. Website

The contact details on the website should be the centre's address, e-mail and telephone number. Staff or childrens' personal information will not be published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Written permission from parents or carers will be obtained before photographs of children are published on the website. This consent form is considered alid for the entire period that the child attends this setting unless there is a change in the child's circumstances where consent could be an issue. Parents/carers may withdraw permission, in writing, at any time.

Photographs that include children will be selected carefully and where photographs are used names will not be included.

Photographs of individual children will not be permitted to be placed on children's 'homepages'. Only pictures of groups or group activities will be permitted.

Children's work can only be published by outside agencies with the permission of the family.

10. Digital and Video Images

Written permission from parents/carers will be obtained and documented before any images of children are recorded. This may mean that separate permissions are needed for:

a. Evidence of EYFS tracking or play quality in the setting.
b. Use of images on setting website or other publicity.
c. Images recorded during events/ parties/ fundraising or outings.

Parents must be made fully aware of how any images of their children may be used or must have the right to decide if they wish their children to be photographed. Parents must be able to have a say in how these photos will be used.

Digital images will be stored in a separate file on the computer, which is accessed by setting practitioners only. These images must be stored in accordance with data protection laws e.g.: password protected files, cameras and memory sticks locked away.

While using digital images, practitioners should be aware of the risk associated with taking, using, sharing, publishing and distribution of images.

Setting practitioners must only use the setting equipment: personal equipment must NOT be used to record images of the children.

Staff should be vigilant when taking digital/video images of the children to ensure that they are appropriately dressed.

Children's full names/names will not be used anywhere on the settings literature

After a photograph is taken down it will be either stored in the child's file, returned to the family or shredded

On the event of parents/carers wanting to take photographs for their own personal use, the Centre will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. performances and assemblies etc. Parents/ carers will be asked to sign a form agreeing to this when attending such events.

11. Games Consoles

Practitioners should ensure that all games consoles and games used are suitable and appropriate for the ages of children in their care.

Use of computer consoles should be supervised and monitored and children encouraged to participate in a broad range of activities.
All games used should be originals and not copies.

Parents/carers should be made aware that computer games are available and have the option to request that their child does not access this equipment.

Children should be closely supervised to ensure that they are not accessing the Internet via the console. Or if they are permitted to do so that the websites accessed are appropriate and the setting has put in place appropriate safeguards.

12. Social networking and personal publishing

The Centre will filter access to certain social networking sites.

Newsgroups will be blocked unless a specific use is approved.

Children and parents will be advised that the use of social network spaces outside the centre is inappropriate for children under the age of 14. However, we accept that some families will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.

Children are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

Practitioners, volunteers, students, registered bodies etc should not put details of their work on any form of social networking site.

Practitioners, volunteers, student, registered bodies etc should not engage in any on-line activity that may compromise their professional responsibilities.

Photographs, names of, or comments about children within the setting must never be placed on any social networking site.

Adults working with children/young people should not correspond with setting's children/families through social networking sites.

Practitioners should be aware of possible implications when entering any personal details on any gaming or social networking sites (e.g. YouTube, Facebook, twitter etc).

The setting's computer/laptop should only be used for setting related activities. Practitioners will not be permitted to use the equipment to access social networking sites at any time, including designated breaks.

All communications in the setting should be transparent and open to scrutiny.

13. Managing filtering

The Centre will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect children are reviewed and improved.

If children or staff discovers an unsuitable site, it must be reported to the Class Teacher, e-Safety Coordinator or Headteacher.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Centre is allowed.

The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.

Staff will use the Centre's phone where contact with family is required.

Staff should not use personal mobile phones during contact sessions

14. Authorising Internet access

All families must sign up to the Acceptable Use Agreement for children and abide by the Centre's e-Safety rules.

Access to the Internet will be by directly supervised access to specific, approved on-line materials.

All parents will be asked to sign the Acceptable Use Agreement for children giving consent for their child to use the Internet in the centre by following the centre's eSafety rules and within the constraints detailed in the centre's e-Safety policy.

All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any centre ICT resource.

Adult users are provided with an individual network, email and login username and password, which they are encouraged to change periodically. .

Staff are aware of their individual responsibilities to protect the security and confidentiality of the centre's network, MIS systems.

The Centre will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a centre computer. Neither the Centre nor Bristol LA can accept liability for the material accessed, or any consequences of Internet access. The Centre will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.

15. Handling e-Safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the e-Safety coordinator. In the event of misuse parents will always be informed.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety coordinator and recorded

Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a child protection nature must be dealt with in accordance with child protection procedures.

Families will be informed of the complaints procedure.

16. e-Safety Training

All staff will be given the Centre e-Safety policy and its importance explained. Training should highlight that:

- Any information downloaded must be respectful of copyright, property rights and privacy.
- Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.

- Laptops issued to staff remains the property of the Centre. Users of such equipment should therefore adhere to centre policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of the centre.

.

17. Monitoring and review

This policy is implemented on a day-to-day basis by all staff and is monitored by the e-Safety Coordinator. This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the e-Safety Coordinator, ICT Coordinator, Designated Child Protection Coordinator, and Governor with responsibility for ICT and Governor with responsibility for Child Protection (e-Safety committee). Ongoing incidents will be reported to the full governing body.

The e-Safety policy will be revised by the e-Safety Coordinator.

18. Appendix

Family Guidelines for Safe ICT and Internet Use

Acceptable Use Agreement for Staff

FAMILY GUIDELINES FOR SAFE ICT and INTERNET USE

We understand that the use of strong language, swearing or aggressive behaviour is not allowed when using the Email etc.

We will not give personal details (like home address, telephone or mobile number), or the personal details of any other person to anyone, or arrange to meet someone unless my parent/carer has given me permission.

We will only download, use or upload material when I have been given the owner's permission.

We will only view, download, store or upload material that is lawful, and appropriate for other users. If I am not sure about this, or come across any potentially offensive materials we will stop viewing.

Please complete and return this form to Reception

Child's Name ______________________________

As the parent or legal guardian of the child above, I give permission for my son or daughter to use the Internet and ICT. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information. I agree to photos of my child to be reproduced on the website and in promotional material according to the guidelines above.

Parent's Name___________________________________

Parent's signature_________________________________

Acceptable Use Agreement
For Staff

The computer system is owned by the centre and is made available to staff to enhance their professional activities including teaching, research, administration and management. The centre's Internet Access Policy has been drawn up to protect all parties – the children, the staff and the centre.

The centre reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. Staff requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the Head Teacher for approval.

- All Internet activity should be appropriate to staff professional activity or the children's education.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

Name

Date Signed