**Kenilworth Nursery School &**

**Whitnash Nursery School**

****



**Information & Communication Technology**

* **E- Safety, Mobile Phones & Social Networking Policy & Guidance**

|  |  |
| --- | --- |
| **Date initial Policy Written** | **May 2014** |
| **Approved by Governors** | **May 2014** |
|  |  |  |  |
| **Revision 1 Due:** | **Date completed:** | **Head teacher** | **Chair of Governors** |
| **Oct 2023** | **Nov 2023** |  |  |

**Section 1: E-SAFETY**

1. **WHY WRITE AN E-SAFETY POLICY?**

1.1 Pupils interact with the Internet and other communications technologies such as mobile phones on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas and social interaction are both greatly beneficial but can occasionally place young people in danger.

1.2 E-safety comprises all aspects relating to children and young people and their safe use of the Internet, mobile phones, smart watches and other technologies, both in and out of nursery. It includes education on risks and responsibilities and is part of the “Duty of Care” which applies to everyone working with children. A national E-Safety drive is being led by the Child Exploitation and Online Protection Centre (CEOP).

1. **WHAT IS E-SAFETY?**

2.1 E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children, young people and adults about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

2.2 The Internet is an open communications channel, available to all. Applications such as the Web, e-mail, blogs and social networking all transmit information over the fibers of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

2.3 Some of the material on the Internet is published for an adult audience and is unsuitable for children and young people. For instance, there is information on weapons, crime and racism that would be more restricted elsewhere. It is important that children and young people are made aware of appropriate behaviour in relation to contacting others and they must also understand that publishing personal information could compromise their security.

2.4 As a Nursery School we need to protect pupils and staff but also to protect ourselves from legal challenge. The law is catching up with Internet developments: it is an offence to store images showing child abuse and to use Internet communication to “groom” children. The Computer Misuse Act 1990(http://www.opsi.gov.uk/acts/acts1990/UKpga\_19900018\_en\_1.htm) makes it a criminal offence to “cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer”.

2.5 We can help protect ourselves by making it clear to pupils, staff and visitors that the use of School equipment for inappropriate reasons is “unauthorised”. However, the Schools are aware that a disclaimer is not sufficient to protect the School from a claim of personal injury and the School needs to ensure that all reasonable actions have been taken to protect users.

**Introduction**

3.1 The Schools have an appointed E-Safety Co-ordinator who is also a Designated Safeguarding Lead as the roles overlap. The named person is Amy Dougherty (WNS) and Christy Aylott-Mayor (KNS).

3.2 Our E-Safety Policy has been written by the School, building on the Warwickshire ICT Development Service E-Safety Policy and government guidance. It has been agreed by the Senior Leadership Team and approved by Governors.

3.3 The E-Safety Policy will be reviewed bi-annually.

**4. WHY IS INTERNET USE IMPORTANT?**

4.1 The Internet is an essential element in 21st Century life for education, business and social interaction.

4.2 The purpose of Internet use in the School is to support the professional work of staff and to enhance the School’s management information and business administration systems.

**5. HOW DOES THE INTERNET ENHANCE LEARNING?**

5.1 Benefits of using the Internet in education include: -

* Access to world-wide educational resources including museums and art galleries;
* Inclusion in the National Education Network which connects all UK schools;
* Vocational, social and leisure use in libraries, clubs and at home;
* Access to experts in many fields for pupils and staff;
* Professional development for staff through access to national developments, educational materials and effective curriculum practice;
* Collaboration across support services and professional associations;
* Improved access to technical support including remote management of networks and automatic system updates;
* Exchange of curriculum and administration data with the LA and DfE;
* Access to learning wherever and whenever convenient.

**6. EVALUATING INTERNET CONTENT**

6.1 If staff discover unsuitable sites, the URL (address), time, date and content must be reported to Warwickshire ICT Development Service 01926 414 100, and where appropriate, the School e-safety officer.

6.2 The Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

**7. MANAGING INTERNET ACCESS**

7.1 The security of the Schools information systems will be reviewed regularly.

7.2 Through Warwickshire ICT Development Service, virus protection will be installed and updated regularly.

7.3 The school uses the Warwickshire Broadband with its firewall and filters.

7.4 The Schools provide an addition level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Service.

7.5 Portable media, separate to that purchased by the Schools may not used without specific permission and a virus check.

7.6 Files held on the Schools network will be regularly checked.

7.7 The Schools Business Manager will review system capacity regularly.

**8. EMAIL**

8.1 Access in the School to external personal e-mail accounts may be blocked.

8.2 E-mail sent to external organisations should be written carefully, in the same way as a letter written on school headed paper.

**MOBILE PHONES & SMART WATCHES**

**9.1** Personal mobile phones and smart watches must not be used to communicate with families/exchange information. The School provides phones for this purpose. If you are contacted by a family on a personal mobile please direct their enquiry to the School Office.

**9.2** Use of mobile phones or smart watches by staff, families or visitors should not be used during session times or be turned on in any teaching and learning spaces except with the permission from the Senior Leadership Team. Staff may use a smart watch as a watch but must disable all other features.

**10. PUBLISHED CONTENT AND THE SCHOOL WEBSITE**

10.1 The contact details on the Website should be the Nursery Schools address, e-mail and telephone number. Staff or pupils personal information will not be published.

10.2 Email addresses should be published carefully, to avoid spam harvesting.

10.3 The Head teacher and Office Managers will take overall editorial responsibility and ensure that website content is accurate and appropriate.

10.4 The Website should comply with the School guidelines for publications including respect for intellectual property rights and copyright.

**11. PUBLISHING STAFF AND PUPIL’S IMAGES AND WORK**

11.1 Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

11.2 Pupils’ full names will not be used anywhere on the Website or social media pages, particularly in association with photographs.

11.3 Written permission from parents or carers will be obtained before photographs of pupils are published on the Schools Website or social media pages. This is usually at the point of admission / registration with the School.

11.4 Pupil’s work can only be published with the permission of the pupil and parents/carers.

11.5 Images of staff and governors should not be published without consent.

**12. SOCIAL NETWORKING AND PERSONAL PUBLISHING**

12.1 Social networking sites and newsgroups will be blocked unless a specific use is approved.

12.2 Parents/carers of pupils should be advised not to place personal photos on any social network space.

They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, nursery school or shopping centre.

12.3 Staff should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. They should be encouraged to invite known friends only and deny access to others.

**13. MANAGING FILTERING**

13.1 The school will work in partnership with the Warwickshire ICT Development Service and Becta who will ensure filtering systems are as effective as possible.

13.2 If staff discover unsuitable sites, the URL, time and date must be reported to the Schools E-Safety Co-ordinator.

13.3 Any material that the School believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

**14. MANAGING EMERGING TECHNOLOGIES**

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

14.2 Mobile phones and smart watches will not be used during sessions, or be located in any teaching spaces. The sending of abusive or inappropriate text messages is forbidden.

14.3 The School should investigate cellular wireless, infra-red and Bluetooth communication and decide a policy on phone use on the premises.

**15. PROTECTING PERSONAL DATA**

15.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

**16. AUTHORISING INTERNET ACCESS**

16.1 All users must read and abide by the “Acceptable ICT Use Policy” before using any School ICT resources.

**17. ASSESSING RISKS**

17.1 The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy monitored.

17.2 The use of computer systems for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

17.3 Methods to identify, assess and minimise risks will be reviewed regularly. For example through the E-Safety Coordinator attending training and the monitoring against the E-Safety quality mark framework.

**18. HANDLING E-SAFETY COMPLAINTS**

18.1 Any complaint about staff misuse must be referred to the Headteacher who should use the agreed WCC procedures.

**19. COMMUNITY USE OF THE INTERNET**

19.1 Community use would be in line with the Schools **“**Acceptable ICT Use” Policy.

**20. STAFF AND THE E-SAFETY POLICY**

20.1 All staff will be given the Schools **“**Information & Communication Technology *(E- Safety & Social Networking Policy & Guidance)” during induction and* its importance explained.

20.2 Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

20.3 All staff should read and sign the Schools **“**Acceptable ICT Use” Policy.

20.4 Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

20.5 Staff development in safe and responsible Internet use in line with the Schools “Information & Communication Technology(E-Safety & Social Networking Policy & Guidance)”.

**21. ENLISTING PARENTS/CARERS SUPPORT**

21.1 Parents/carers attention will be drawn to the Schools “Information & Communication Technology (E-Safety & Social Networking Policy & Guidance)” in newsletters, the School prospectus and on the Schools Websites.

21.2 Internet issues will be handled sensitively to inform parents/carers without alarm.

21.3 A partnership approach with parents will be encouraged. This could include parents/carers evenings with demonstrations and suggestions for safe home Internet use.

21.4 Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

21.5 Interested parents/carers will be referred to organisations listed in section 3 E-Safety Contacts and References.

**Web Links *Becta has produced these booklets that are essential reading:***

• Safeguarding children in a digital world (Feb 2006) Ref: BEC1-15401

• E-safety: Developing whole-school policies to support effective practice (revised Feb 2006) Ref: BEC1-15402

• Signposts to safety at KS1 and KS2 (April 2007) Ref: BEC1-15488

• Signposts to safety at KS3 and KS4 (April 2007) Ref: BEC1-15489

• Using technology safely in schools – an essential guide (April 2007) Ref: BEC1-15461

• AUPs in context: Establishing safe and responsible online behaviours (February 2009) *Ref: BEC1-15648*

|  |  |
| --- | --- |
| ***Useful E-safety programmes include:*** • Think U Know www.thinkuknow.co.uk • Childnet www.childnet-int.org/kia • Kid Smart www.kidsmart.org.uk/ • The BBC’s Chat Guide www.bbc.co.uk/onlinesafety/ • CBBC Stay Safe www.bbc.co.uk/cbbc | ***E-Safety Contacts and References:*** Warwickshire ICT Development Service Desk 01926 414100 Child Exploitation & Online Protection Centre http://www.ceop.gov.uk/contact\_us.html Virtual Global Taskforce – Report Abuse - http://www.virtualglobaltaskforce.com/ Think U Know website http://www.thinkuknow.co.uk/ Becta http://www.becta.org.uk/schools/safety Internet Watch Foundation <http://www.iwf.org.uk/> Internet Safety Zone http://www.Internetsafetyzone.org.uk/ KidSMART http://www.kidsmart.org.uk/ NSPCC http://www.nspcc.org.ukChildline http://www.childline.org.uk/ NCH – The Children’s Charity http://www.nch.org.uk/storiesCBBC Safe Surfing including the Chat Guide http://www.bbc.co.uk/cbbc/help/safesurfing/ The Warwickshire Safeguarding Children Board have provided guidance and contacts in their publication, *Keeping Children Safe and Healthy* (“The Blue Book”), should you be concerned about the Internet usage of a child, young person or member of staff.http://www.warwickshire.gov.uk/Web/corporate/pages.nsf/Links/ D45A0720FD40CFC580256EE4004C6C70  |

**Section 2: Social Networking**

**Policy on Staff/Governor Use of Social Networking and Internet Sites**

1. **Introduction**
	1. Social media includes online social forums such as Facebook, Twitter and LinkedIn and websites such as YouTube and Flickr. This type of media which is now widely used allows people to communicate instantly and share data in a public forum.
	2. This Policy sets out the School’s approach to staff use of social media and internet sites and action that may be taken when it is considered a member of staff may have breached this Policy.
	3. There are many more examples of social media than can be listed here and this is a constantly changing area. Staff should comply with this Policy in relation to any social media that they use.
	4. The term “staff” in this document, should also be read to include any contractors or volunteers at the school. There is a separate section in relation to school governors towards the end of this document.
	5. In using social networking and internet sites, clear and explicit professional boundaries will be adhered to as outlined in Section 12 of ‘Guidance for Safer Working Practice for those working with Children and Young People in Education Settings’ (Safer Recruitment Consortium 2015), which can be found at the following link <http://www.saferrecruitmentconsortium.org/GSWP%20Oct%202015.pdf>
2. **Objectives**
	1. The purpose of this policy is to:
	2. Clarify what the School considers to be appropriate and inappropriate use of social networking and internet sites by staff;
	3. Encourage social networking/internet sites to be used in a beneficial and positive way;
	4. Safeguard staff, pupils, parents/carers and members of the public from abuse on social networking sites;
	5. Safeguard the reputation of this School; other schools; the Local Authority and other organisations, from unwarranted abuse on social networking sites;
	6. Set out the procedures that will be followed where it is considered that staff have inappropriately or unlawfully used social networking/internet sites.
3. **Personal use of social media at work**
	1. Staff are not allowed to access social media websites from the School's computers or devices at any time for personal use. [This includes [laptop/palm-top/hand-held] computers or devices distributed by the School for work purposes.]
	2. The School has specifically blocked use of some social media websites on its computers and may at its discretion block further sites.
	3. The School understands that staff may wish to use their own computers or devices, such as laptops and palm-top and hand-held devices, to access social media websites while they are at work. Staff must limit their use of social media on their own equipment to their official rest breaks (such as their lunch break) and must still ensure that they continue to follow the requirements set out in this Policy.
	4. If it is believed a member of staff has engaged in unlawful activity on a social media site or activity in breach of this Policy and the Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings, Section 12, communication with pupils (see link in 1.5) an investigation will be instigated which may result in disciplinary action and potentially dismissal. The School’s disciplinary policy will be followed.
	5. **Use of social media and the internet for work purposes**

In specific circumstances it may be appropriate for a member of staff to use social media as part of their work. For example, as an administrator of the Schools ‘Facebook’ page. This should only take place with the [written] approval of the head teacher / or it is within a job description.

In such circumstances while contributing to the School's social media activities the same safeguards must be adhered to as would be with any other form of communication about the School in the public domain. Any communications made in a professional capacity through social media, either through the post made or a member of staffs response to it must not either knowingly or recklessly:

* + Place a child or young person at risk of harm;
	+ bring the School into disrepute;
	+ breach confidentiality;
	+ breach copyright;
	+ breach data protection legislation; or
	+ do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by: making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;using social media to bully another individual; or posting images that are discriminatory or offensive or links to such content.
1. **Excessive use of social media/internet at work**
	1. Staff must not spend an excessive amount of time while at the School on personal use of social media or internet sites. Rest breaks / lunch times are the only permitted occasions for personal use of social media. They must ensure that use of social media/internet does not interfere with their duties.
2. **Monitoring use of social media/internet on school equipment during work time**
	1. The School reserves the right to monitor staff internet usage. The School considers that valid reasons for checking internet usage include concerns that social media/internet sites have been accessed in breach of this Policy.
3. **Inappropriate use of social media/internet**

The following list gives examples of use of social media/internet sites that the school may consider to be inappropriate:

* 1. Publishing defamatory; discriminatory; illegal; sexual; racist or other offensive material;
	2. Publishing any material which is confidential or would breach copyright or data protection principles;
	3. Promoting personal financial interests, commercial ventures or personal campaigns in school time;
	4. Publishing anything of an abusive or harassing nature;
	5. Using social media/internet sites in a manner that would put staff/governors in breach of school codes of conduct or existing policies
	6. Discussing matters relating to school, staff, pupils or parents/carers for which the social media is not considered to be an appropriate forum and is likely to lead to disciplinary action
	7. Inappropriately holding yourself out as, or implying that you are, a representative of the school when using social media/internet sites in a private context;
	8. Interacting with pupils via social media/internet sites [*unless properly authorised as part of school duties];*
	9. Interacting with parents/carers of pupils via social media/internet sites
	10. Interacting with any ex-student who is under the age of 18 (staff should exercise extreme caution in interacting with any ex-pupils regardless of age);
	11. Actively providing false or misleading information about the school, its staff or pupils;
	12. Cyber-bullying
	13. Inappropriately referencing other staff members, governors, students, parents/carers or school activities/events - unless it is a legitimate part of the staff member’s role
	14. Using social media/internet sites to raise complaints/grievances – any issues should be raised via the appropriate channels (e.g. school complaints procedure).

The above is a non-exhaustive list. It is intended to provide some examples of what the School considers to be inappropriate. Each matter will be dealt with based on its own facts. School policies will be followed where relevant (e.g. the School’s disciplinary/bullying /complaints policy etc). The School will contact the Police where it is necessary to do so.

1. **Social media in your personal life**
	1. The School recognises that many people make use of social media in a personal capacity. While they are not acting on behalf of the School, staff must be aware of the potential damage that could be caused to the School if they are recognised as being a member of staff.
	2. Staff may say that they work for the School but their online profile (for example, the name of a blog or a Twitter name) must not contain the School's name.
	3. If staff do discuss their work on social media (for example, giving opinions on their specialism or the sector in which the School operates), where appropriate they should include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of the School."
	4. Any communications that staff publish in a personal capacity through social media must not bring the School into disrepute.
	5. Any behaviour / images that staff publish in a personal capacity through social media must not bring the School into disrepute.
	6. No member of staff should interact / connect with any families whose children attend the school, or who have attended the school, or may do so on the future, on social networking sites. If staff member has a family member/friend whose child attends the school they are to inform SLT.
2. **Disciplinary action over social media use**
	1. All staff are required to adhere to this policy. Staff should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the School, may constitute gross misconduct and lead to summary dismissal.
	2. Similarly, where there is a serious breach of this policy, action may be taken in respect of other members of staff who are not employees which may result in the termination of their appointment.
	3. Staff have a duty to report abuses of this policy in accordance with the schools whistleblowing policy.
3. **Child protection guidance**
	1. If the head teacher (*or other member of staff*) receives a disclosure that a member of the School’s staff is using a social networking/internet site in a way that may put a child at risk, this should be recorded in line with the School’s child protection policy and whistleblowing policy as an allegation. In accordance with *the Department for Education’s (DfE)* [Working Together to Safeguard Young People (2015)](http://media.education.gov.uk/assets/files/pdf/w/working%20together.pdf), the head teacher will refer all allegations of a safeguarding nature to the Designated Officer (DO) in the Local Authority before undertaking any internal investigations. [*Designated Officer – Children and Families Front Door on 01926 414144 or*  mash@warwickshire.gov.uk].
4. **Staff/governors interacting with each other online**
	1. Governors are advised not to be “friends” with members of staff online. Reasons for this include:
* Potential for a conflict of interest where a governor is on a selection panel/disciplinary panel where a “friend” is involved
* Due to the role of the governing body and its general responsibility for the conduct of the school, it is sensible to maintain a certain level of separation between governors and staff.
* If a governor is a friend of a staff member on social media they are to inform the Head of Federation.
	1. Teachers and other staff members should also exercise caution when considering inviting work colleagues to be ‘friends’ on social networking sites, as this may create a conflict/difficult situation in the future.
1. **Application of this Policy to school governors**
	1. Whilst some aspects of this Policy are clearly more targeted at school staff, many have equal application to governors. For example, section 7 of the Policy provides guidance for all on what is considered to be inappropriate use of social media/internet sites. All governors should ensure that they comply with the spirit of the Policy.
	2. Though governors would not be subject to the same disciplinary process as staff, there are still forms of redress available where a governor behaves in an inappropriate manner. The appropriate procedures would be followed in such cases.
2. **Involvement with the PTA**

This policy will continue to apply to members of staff who are acting in their capacity as a member of Parent-Teacher Association (PTA) where one exists. Therefore they should ensure that they are acting in the spirit of this policy when acting in this capacity.

1. **Requirements for staff on using social networking**
* No member of staff should interact with any pupil in the school on social networking sites
* No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18
* This means that no member of the school staff should request access to a pupil’s area on the social networking site. Neither should they permit the pupil access to the staff members’ area e.g. by accepting them as a friend.
* No member of staff should interact / connect with any families whose children attend the school, or who have attended the school, or may do so on the future, on social networking sites. However if they are friends or family of the staff member, they are to inform the headteacher or SLT.
* Where family members have pupils in school and there are legitimate family links, please inform the Head Teacher in writing. However, it would not be appropriate to network during the working day on school equipment
* It is illegal for an adult to network, giving their age and status as a child
* If you have any evidence of pupils or adults using social networking sites in the working day, please contact the designated Child Protection person in the school

**14. Cyber Bullying**

By adopting the recommended no use of social networking sites on school premises, Atherstone and Bedworth Heath Nursery School & WEYH protect themselves from accusations of complicity in any cyber bullying through the provision of access.

Parents/carers should be clearly aware of the school’s policy of access to social networking sites.

Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school.

This can be a complex area, and this example might help:

*A child is receiving taunts on Facebook and text from an ex pupil who moved three months ago: This is not a school responsibility, though the school might contact the new school to broker a resolution.*

**Smart Watches**

At Kenilworth and Whitnash Nursery School Federation, the welfare and well-being of our children is paramount. The aim of the updates to policies is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice through establishing clear and robust acceptable mobile user guidelines. This is achieved through balancing protection against potential misuse with the recognition that mobile phones and smart watches are effective communication tools.

This updated policy applies to all individuals who have access to smart watches on site. This includes staff, volunteers, Governing Body, children, young people, parents, carers, visitors, and contractors. This list is not exhaustive.

**Smart Watches**

* Staff/Volunteers/ Visitors are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office.
* **Smart watches can be worn during the school day in all areas of school, but the camera, messaging and call services must be disabled (this is easy to do and, on most watches, will be one button).**
* During lunch breaks, staff can enable their smart watch in environment spaces that do not have children in them etc staff room, office space. Watches MUST be then disabled for camera, messaging and call services, once lunch breaks are finished.
* Staff **are not** at any time permitted to use recording equipment on their smart watches, for example: to take recordings of children. Legitimate recordings and photographs should be captured using school equipment such as cameras and iPads.
* Staff should report to the Head Teacher or a member of SLT any usage of smart watches that do not meet the updated policy that is detailed above.

**Review**

This policy will be reviewed annually. This policy was adopted by the Governing Body at its meeting on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# I have read and understood and agree to comply with the School’s Policy on Staff Use of Social Media/ Internet Sites.

Signed: ……………………….............

Print name:……………………………

Date: ………………