Online safety

This online safety policy has been written by Nisha Reed, involving staff, committee, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2021, Early Years and Foundation Stage 2021, 'Working Together to Safeguard Children' 2020 and the Kent Safeguarding Children Multi Agency Partnership (KSCMP) procedure.

This policy applies to all staff including the committee, management and administration team, teachers, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers. This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. See Privacy Notice for parents and staff.

Policy statement

We take steps to ensure that there are effective procedures in place to protect children, young people and vulnerable adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting.

Our designated person responsible for co-ordinating action taken to protect children is Nisha Reed, Designated Safeguarding Lead (DSL)

The setting identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care, for example, bullying, grooming, radicalisation, or abuse of children and learners.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

- NWPS will ensure that all staff receive online safety training as part of their induction and that ongoing online safety training and update for all staff will be integrated, aligned and considered as part of our overarching safeguarding approach.

It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

It is the responsibility of parents and carers to:

- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Procedures

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used by staff and children.
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- All computers have virus protection installed.
- The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.

Internet access

- Children do not normally have access to the internet and never have unsupervised access.
- If staff access the internet with children for the purposes of promoting their learning, written permission is gained from parents who are shown this policy.
- The designated person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.
- Children are taught the following stay safe principles in an age-appropriate way prior to using the internet.
  - only go online with a grown up
  - be kind online
  - keep information about me safely
  - only press buttons on the internet to things I understand
  - tell a grown up if something makes me unhappy on the internet
- Designated persons will also seek to build children's resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
- If a second-hand computer is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it.
- All computers, for use by children, are located in an area clearly visible to staff.
- Children are not allowed to access social networking sites.

Email

- Children are not permitted to use email in the setting.
- Parents and staff are not normally permitted to use setting equipment to access personal emails.
- Staff do not access personal or work email whilst supervising children.
- Where staff send personal information by email, this information is shared securely at all times, for example, with the use of password protected documents.
- Staff and committee use business emails for work related communication with external bodies.

Mobile phones and smart

watches – children

- Children do not bring mobile phones, smart watches, or other ICT devices with them to the setting. If a child is found to have a mobile phone, smart watch or ICT device with them, this is removed and stored securely until the parent collects them at the end of the session. *Please see our Mobile Phones and Camera Policy*

Social media

The expectations' regarding safe and responsible use of social media applies to all members of Nettlestead and Wateringbury Preschool and Out of Schools Club community. The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

  - Setting the privacy levels of their personal sites.
  - Being aware of location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Keeping passwords safe and confidential.
  - Ensuring staff do not represent their personal views as that of the setting.

- Staff are advised not to accept service users, children and parents as friends due to it being a breach of expected professional conduct. If a practitioner and family are friendly prior to the child coming into the setting, this information is shared with the managers prior to a child attending and a risk assessment and agreement in relation to boundaries is agreed.
- In the event staff do name the organisation or workplace in any social media they do so in a way that is not detrimental to the organisation or its service users.
- Staff observe confidentiality and refrain from discussing any issues relating to work.

- Members of staff are encouraged not to identify themselves as employees of Nettlestead and Wateringbury Preschool and Out of Schools Club on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework and may have an impact on Ofsted inspections.
- Staff do not upload comments or photographs of company events without permission from the managers and colleagues.
- Staff avoid personal communication, including on social networking sites, with the children and parents with whom they act in a professional capacity.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL.
- Staff should report any concerns or breaches to the designated person in their setting.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the managers immediately if they consider that any content shared on social media sites conflicts with their role.

If your online presence references your employer, please consider that personal blogs, comments posted on other blogs, forums, and social networking sites should:

- Refrain from comment that can be interpreted as slurs, demeaning, inflammatory etc. and must not publish any views which are discriminatory or narrow-minded.
- Be clear and write in first person.
- Have clear disclaimers that the views expressed by the author of the blog are the author's alone and do not represent the views of the Company.
- Make it obvious in your blog that you are speaking for yourself and not on behalf of the Company.
- Comply with the Company's confidentiality and disclosure of proprietary data policies.
- Be respectful to the Company, other employees, customers, partners and competitors.

If you are unsure about whether a blog, tweet, post, comment, or photo is acceptable, always consult your managers. Employees should understand that the employer has the right to monitor the use of social media and social networking websites, even if they are engaging in social networking or social media use away from the office. Inform your managers of any blogs to which you regularly contribute.

Use and/or distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately, the Safeguarding Children and Child Protection policy, in relation to allegations against staff and/or responding to suspicions of abuse, is followed
- Staff are aware that grooming children and young people online is an offence in its own right and concerns about a colleague's or others' behaviour are reported (see Whistleblowing Policy).

A breach of any of the above is considered by the Company to be a disciplinary matter and may result in disciplinary action being taken against the offending employee.

Employees should not contact the media with allegations about the Company.

Official Use of Social Media

- Nettlestead and Wateringbury Preschool and Out of Schools Club official social media channels are:
  Parents of NWPS close Facebook group - https://www.facebook.com/groups/169807316879400/
  Public Facebook - https://www.facebook.com/NettlesteadandWateringbury
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- The official use of social media as a communication tool has been risk assessed and approved by the managers and committee.
- Management staff and committee have access to account information and login details for our social media channels.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
- Official social media sites are suitably protected and, where possible, run and/or linked to/from our website.
- Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including anti-bullying, image/camera/smart watch use, data protection, confidentiality and child protection.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

- Any official social media activity involving learners will be in-line with current policies.

Managing the Safety of our Website

- We will ensure that our website complies with guidelines for publications including accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.

Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, and procedures including the setting Whistle Blowing Procedure.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy DSL's) will seek advice from the Education Safeguarding Service.
- Where there is suspicion, that illegal activity has taken place, we will contact the Education Safeguarding Service or Kent Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or headteacher/manager will speak with Kent Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

Concerns about Learners Welfare

- The DSL (or deputy DSL's) will be informed of any online safety incidents involving safeguarding or child protection concerns.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.
- The DSL will record these issues in line with our child protection policy, following local and national advice guidelines. (See additional information)
- The DSL (or deputy DSL's) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the managers who will report it to the Internet Watch Foundation at www.iwf.org.uk
- Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk

- If staff become aware that a child is the victim of cyber abuse (peer on peer abuse issues, such as bulling and sexting) they discuss this with their parents and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk
-

Staff Misuse

- Any complaint about staff misuse will be referred to the managers, in accordance with the allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff Code of conduct and Disciplinary and Grievance Procedures.

Kent Support and Guidance for Educational Settings

Education Safeguarding Service:

- Rebecca Avery, Education Safeguarding Advisor (Online Protection)
- Online Safety Development Officer
- Tel: 03000 423164

Further guidance for Educational Settings:

- www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
- www.theeducationpeople.org/blog/?tags=Online+Safety&page=1
- UKCIS UK Council for Internet Safety - GOV.UK (www.gov.uk)

KSCMP: www.kscmp.org.uk

Kent Police: www.kent.police.uk or www.kent.police.uk/internetsafety

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

This policy was adopted at a meeting of	
	NWPS
Held on	
Date to be reviewed	May 2024

Signed on behalf of the provider _____

Name of signatory _____

Role of signatory (e.g. chair, director or owner) _____

_____

Useful Links for Educational Settings

Kent Support and Guidance for Educational Settings

Education Safeguarding Service:

- Rebecca Avery, Education Safeguarding Advisor (Online Protection)
- Ashley Assiter, Online Safety Development Officer
    - Tel: 03000 415797
- Guidance for Educational Settings:
    - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
    - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
    - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
    - www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCMP:

- www.kscmp.org.uk

Kent Police:

- www.kent.police.uk

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Other:

- Kent Public Service Network (KPSN): www.kpsn.net
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources for Educational Settings

- CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk
- Childnet: www.childnet.com

- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk