Bentilee Nursery School E-Safety Policy
(to be read in conjunction with Social Media Policy)

Reviewed: October 2024
Next review: October 2025
Personnel: Headteacher, Early Years Practitioners, teacher, office manager, TSAs, family support worker, Governing body.

Writing and reviewing the e-safety policy

The school's e-safety coordinator is Jayne Grindey. She liaises daily with Nicola Hill (deputy safeguarding lead) regarding any safeguarding concerns. Jayne Grindey is also the ICT coordinator as the roles overlap. The e-safety governor is Ann Harvey. She will act as a critical friend termly. All staff have an equal responsibility. The ultimate responsibility will be the Headteacher. Our e-safety policy has been written by the school, building on the Stoke on Trent e-safety policy and government guidance. It has been agreed by the senior management and approved by governors. The authority has a website www.safeguardingchildren.stoke.gov.uk which is kept updated.

EVOLVE is the company we use to provide the internet monitoring and filtering

Teaching and Learning

The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Staff should guide pupils in on line activities that will support the learning outcomes planned for the pupil's age and maturity.

Staff will be taught how to evaluate internet website appropriate and age suitability.
The school will ensure that the copying and subsequent use of the internet derived materials by staff and pupils complies by copyright law.

Pupils will be taught how to stay e-safe
Curriculum planning will include age appropriate opportunities to discuss and role play. Stories e.g. feelings/emotions will be read, and children will learn about

the benefits and risks offered by new technologies.
We support parents in making decisions about e-safety (with at least an annual workshop for parents).

Managing Internet Access

Information system security

Virus protection will be updated regularly on all networked computers.
School ICT systems capacity and security will be reviewed regularly.
Supervision of pupils will be at all times.

Wi-fi access is turned OFF on children's IPADS to prevent pop ups.

When in use, apps are locked into place using the guided access function as described below:-

Accessibility – Guided access ON – The passcode applied – Desired app accessed – Home button tapped xxx times to turn on access – Home button tapped xxx times to turn off guided access.

E-mail

Staff may only use approved e-mail accounts on the school system. The office manager will be responsible to ensure all new members of staff have an account and old staff are deleted.

Staff have signed an e-safety agreement to ensure child assessments completed on ipads are only used for school work and nothing from them is to be used for personal use or emailed in any capacity.

Public web published content and the school website

The content details on the website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

Web publishing pupil's images and work

Images, published to the web, that include pupils will be selected carefully and with written permission of parents/carers. This is reviewed at each new intake. No image is uploaded / published until a new exclusion list has been compiled.

Pupils full names of children will not be used anywhere on the website, particularly in association with photographs.

Social networking and personal publishing – see Social Networking protocol policy for full information.

The /school will block/filter access to social networking sites, except those specifically purposed to support educationally approved practice.
New groups will be blocked unless a specific use is approved.

Staff must never to give out personal details of any kind which may identify them or their location.

Staff must not publish specific and detailed private thoughts on social networking sites.

Parents and staff are reminded not to upload photos they have taken at any celebrations (e.g the Christmas play, daily activities, after school clubs, Mother's day and Leavers assembly etc.), onto Facebook or any other social media site as they might contain images of other children, staff, parents and volunteers and compromise the school.
At the event they sign to say they have understood this.

Staff are reminded that parents who have been friends from staff distant past must not be friends on Facebook/ other social media sites, as this could lead breech school's confidentiality or bring the school into disrepute.

Mobile phones- No one can use their mobile phones in the school around children.(for further information – see mobile phone policy)

Staff, parents, volunteers, visitors, contractors in the school day, at afterschool clubs, on consultations with staff or staying for "stay and plays" must not to use their mobile phones in school to safeguard against children's images being misused.

In times of emergency staff / volunteers/ parents can leave their mobile phone in the office on and will be alerted when it rings for them.

Managing filtering
The school has a filtering box installed by EVOLVE called **sonic wall** to ensure systems protect pupils are reviewed and improved. It filters and stops people being able to hack into the school network. We also use forensic software which helps us to **monitor** any wrong usage e.g. sites and emails using inappropriate words. EVOLVE alert us with any incidents.

If overblocking occurs (restricts access to non harmful pages that could be used in an educational context) staff must speak to the Designated

safeguarding lead, who will speak to EVOLVE for access.

If staff or pupils discover an unsuitable site, the URL must be reported to the Head teacher or office manager Sue Ridgway, to allow us to contact our IT support company EVOLVE.

The school gets alerts if there shows that a site has tried to be opened that is blocked by the filtering system or if an email contains a word that is deemed inappropriate.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out, and protocols established before use in school is allowed.
Mobile phones (cameras on phones) will not be used during lessons or formal school time, unless specifically allowed to support learning as is identified by the teacher. The sending of abusive or inappropriate text messages is forbidden. (in line with mobile phone policy).

Ipads are kept in school but they may be taken home at times to update records. Staff have been made aware of the need to only use them as appropriate for school work and to keep away from children. Staff understand that false use will result in serious consequences and may involve a criminal investigation or conviction.
Any school technology taken off site must be signed in and out.

Policy Decisions

Authorizing internet access
The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications, which includes internet access. The record will be kept up to date, for instance a member of staff may leave or a pupil's access will be withdrawn.
All staff must read and sign the 'Staff information's systems code of conduct' before using any school ICT recourse. (see section 6) included in policy and appendix.
In the nursery access to the internet will be an adult demonstration or by directly supervised access to specific, approved online materials. We have forensic logs on our computers to monitor inappropriate use.

Assessing risks
The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet contents, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Stoke on Trent city council can accept liability for the material accessed, or any consequences of internet access.

Any complaint about staff misuse must be referred to the Head teacher.

Staff and the e-safety policy
All staff will be given the school e-safety policy and its application and importance explained.
All staff will be informed that all computer and internet will be monitored discretion and professional conduct is essential.
Staff training and safe and responsible internet use and on the school e safety policy will be provided as required.
Staff are responsible for any content on a school laptop. Personal technology e.g. mobile phones should only be used by staff at break times in the staff room or off site.
All staff are informed that social networks will be monitored.

All staff, if they take a device home to communicate with parents know they can ***only add sites to Dojo or Facebook at schoo****l to ensure they are covered by the filtering system.*

- This runs in conjunction with the school Policy on **safeguarding**
- This runs in conjunction with KCSIE 2024 and Working together to safeguard children 2023

Staff information system -Code of conduct- e safety

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this Code of Conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I will not use my personal phone/ camera/ipad/lap top/desktop in school to take photographs or video and will only be allowed in the nursery by permission e.g emergency calls
- I will not use the i-pad/lap top/desk top copmuter for personal use and ensure that data is kept secure and is used appropriately, whether in school or taken off the school premises.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils/ parents are compatible with my professional role.
- I will not publish any content which might put myself or the school in a compromising situation, breech the school's confidentiality in any way or bring the school's reputation into disrepute.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- I will report any e-safety concerns using the Online Incidents report sheet and pass on to Juliet Levingstone. **I have read, understood and agree with the Information Systems Code of Conduct.**

Signed: …… PRINT: …… Date: ……

Accepted for school: …… PRINT: ……

Signing in and out register for IPADs and media

ICT resource to be logged out	Resource	Date taken out	Staff signature	Date returned	Staff signature	Countersigned by