Wentworth Nursery School and Children's Centre

Online safety Policy

To be reviewed

October 2020

Online Safety Policy statement

The aim of this policy is to ensure children, staff, Governors, students and volunteers use the School's internet and Information and Communication Technology (ICT) safely and appropriately and so ensuring the best possible outcomes for our children.

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 and inappropriate language)
- 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
- cyber-bullying in all forms
- identity theft and sharing passwords

Conduct:

- privacy issues, including disclosure of personal information
- digital footprint
- 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 (no thought or consideration for intellectual property and ownership – such as music and film)

Scope

This policy applies to all members of Wentworth Nursery School and Children's Centre community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Wentworth Nursery School and Children's Centre. See appendix for description of roles and responsibilities.

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ staffroom
- Policy to be part of school induction pack for new staff
- School will provide a 'Safe Internet' page for parents on the school website. Information will include internet safety, home web filtering tips and links to e-safety websites
- Acceptable Use agreements discussed with families at the start of each year
- Acceptable Use agreements to be held in pupil and personnel files
- Children and teachers will be provided with training in the area of online safety

Handling complaints:

- The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access.
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - interview/counselling by Online Safety Coordinator / Headteacher;
    - informing parents or carers;
    - removal of internet or computer access for a period;

- referral to Local Authority / Police.

- Our Online Safety Co-ordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Behaviour Policy. Complaints related to child protection are dealt with in accordance with the school and Local Authority child protection procedures.

Review and Monitoring

The online Safety Policy is referenced from within other school policies: Safe Guarding and Behaviour policy.

- The Online Safety policy will be reviewed biennially
- There is widespread ownership of the policy and it has been agreed by the Leadership Team and approved by Governors and the staff team. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

1. Internet access

School's Internet Service Provider is Talk Talk.

2. Email access

School uses Hackney Learning Trust (Microsoft Exchange) to detect and block viruses, spam, (phishing), Trojan, and other malicious message types, and inappropriate language.

We:

a. use standard school-issued email addresses
b. staff and volunteers will use only a school-issued email account for their professional use
c. Staff, volunteers, Governors and all those connected professionally with school will not send material that is illegal, obscene, upsetting or defamatory, or that is intended to annoy or intimidate another person. Should such content be received, it must not be forwarded to anyone, and must be reported to the e-safety co-ordinator, who will take appropriate action
d. know that spam, Trojan and virus attachments are a danger to the school's systems

3. Digital and video images

a. We gain written parental/carer permission for use of digital photographs or video involving their child as part of the agreement form when their child joins Wentworth Nursery School and Children's Centre
b. Digital images/videos of children are only stored on the school's server for teaching and learning purposes which is only accessible to school staff.

4. Equipment

All computer equipment is installed professionally and meets health and safety standards. Equipment is maintained to ensure health and safety standards are followed.

5. Data security

a. Personal data is stored securely. Access to personal data is strictly controlled by both the Head Teacher and School Bursar. Personal data is stored on the school's secure server.
b. Data is secured against loss through systems failure, theft and damage. All data stored on computers are password controlled. Data relating to school business is only used on school laptops and iPad.
c. If sensitive data, defined as being covered by the Data Protection Act, needs to be transferred, it is done so securely. Data is password protected, and the password will be transmitted separately.
d. The use of electronic equipment off-site must be formally approved, in writing, by the user's line manager. There is a school file to sign equipment out, authorised by the HT or DHT.
e. Data security incidents must be reported through the appropriate internal management channels as quickly as possible after the incident or awareness of the incident

f. All electronic equipment that is to be reused or disposed of will have all of its data and software erased/destroyed
g. Data security is reviewed annually, and staff updated annually

6. Named Online Safety lead is Farzana Chowdhury– roles and responsibilities

In the absence of our online safety lead, responsibilities will be addressed by the Headteacher.
A named online safety lead is crucial to developing and maintaining an e-safety culture within the early years setting.
The responsibilities of this role are to:

a. Develop an e-Safety culture at Wentworth Nursery School and Children's Centre
b. Be the named point of contact on all e-safety issues
c. Ensure online-safety is included as part of the induction procedures and the acceptable use of electronic equipment and use of social media will be signed by all staff and volunteers.
d. Monitor online-safety, such as:
    1. ensuring the infrastructure of technology provides a safe and secure environment for children, for example by ensuring filters and other software security are in place
    2. maintaining an e-safety incident log to record concerns and incidents
e. reporting on e-safety issues to the management team and governors.
f. Ensure that all staff, volunteers, parents and governors know what to do if they are concerned about online-safety issue
g. Keep abreast of developing online-safety issues via:
    a. http://www.saferinternet.org.uk/
h. Ensure that e-safety is embedded within continuing professional development (CPD) for staff and volunteers, and co-ordinate training as appropriate.
i. Ensure that e-safety is embedded across all activities as appropriate
j. Ensure that e-safety is promoted to parents/carers, children and others in the setting, the home and the community
k. Review and update e-safety policies and procedures on a regular basis and after an incident

7. Online-Safety and use of digital devices

At all times, children, staff, Governors, Parents, students and volunteers will treat others with respect and will not undertake any actions that may bring the school into disrepute.

At all times, children, staff, Governors, Parents, Students and volunteers will not promote any extremism as highlighted in the Prevent Strategy 2015.

Mobile phones, tablets and other digital devices can present a number of problems when not used appropriately:

a. Mobile/smartphones and personal devices can allow wireless and 3G/4G internet access via alternative ISPs, and therefore bypass the school's central security settings and filtering.
b. Mobile/smartphones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of children or staff.

8. Mobile phones:

a. Staff should not have personal mobile phones with them when they are working with children at the setting. This also applies to students and volunteers.
b. Staff mobile phones must be kept in staff lockers and used only when staff are on break time in the staff room or outside the setting.
c. Staff are not permitted to use their own personal phones or devices for contacting children and their families within or outside of the setting in a professional capacity.
    1. The telephone number of the school should be used by staff in all communication with families, and for emergency contact.
d. Keeping mobile phones in rooms while working with children constitutes a staff disciplinary matter, and may lead to student and volunteers' placement being terminated.

e. Parents, carers and visitors are requested not to use their mobile phones while on the school premises. School staff will remind parents, carers and all visitors of the policy by reminding them to switch off their phones when they enter the setting or asking them to leave the rooms to make or receive calls in the reception area/foyer when necessary.

9. Digital cameras

a. Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils, and will only use work-provided equipment for this purpose.
b. We gain written parental/carer permission for use of digital photographs or video involving their child as part of the agreement form when their child joins
c. Children can only be photographed if permission of parents/carers is given.
d. Personal cameras are not allowed in the setting and should not be used on off-site activities, home visits and outings
e. The setting holds a number of digital cameras for staff and, where appropriate, for parents, carers, students and volunteers to take photographs of children for display, observations or profile books.
f. Use of video equipment can be a legitimate learning/training aid. Children and parents/ carers should be made aware that this is part of the learning/training.
g. Students, volunteers and visitors are not permitted to take photographs or recordings of the children without permission from the Head Teacher or deputy head.
h. No one is permitted to photograph or record images in the toilet and changing areas
i. Photographers will be required to have clear formal identification which must be worn at all times, for example at an open day or event.
j. Children's images will not be used for promotional or press releases unless parents/carers have given prior written consent.

10. Use of ICT equipment

Children should never be allowed to use the internet in the setting without adult supervision

Staff who use the centre's ICT and communications systems:

a. Must sign an Acceptable Use Policy
b. Must use the systems responsibly and keep them safe
c. Must maintain safe professional boundaries with parents. This includes not giving their personal email address to school users or befriending school users on social network sites such as Facebook
d. Must treat as confidential any passwords provided to allow access to all ICT equipment
e. Must report known breaches of this policy, including any inappropriate images, messages or other material which may be discovered on the school's ICT systems
f. Must not install software on the centre's equipment, including freeware and shareware
g. No personal devices (e.g. USB memory sticks) should be used to upload or download material onto the school network or website, or any ICT device.
    1. The school provides encrypted USB memory sticks for staff to use.
h. Use of cloud storage systems (e.g. Dropbox) must be approved by either the e-safety coordinator/ Deputy Headteacher or Headteacher
i. Must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures
j. Must ensure that the systems are used in compliance with this e-safety policy
k. Staff, volunteers and parents will be provided with training in the area of online safety

11. Internet and social networking sites

World Wide Web

a. Internet access at school will always be overseen by a member of staff.
b. Access to websites for children are limited by those agreed by the school only.

c. School staff and volunteers will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials on school equipment

d. School staff will report accidental accessing of inappropriate materials in accordance with school procedures

e. Staff, volunteers and children will use the Internet for educational purposes only

f. The school will NEVER disclose or publicise personal information relating to children on any social media platform

g. Downloading materials or images not relevant to teaching and learning is in direct breach of school policy

h. Staff are instructed not to create or manage social network spaces for pupil use on a personal basis, or to open up their own personal spaces to their pupils or the pupils' families.

i. Staff must not search for, monitor or investigate social networking presences of pupils or families.

    1. If a staff member does happen to find such a social network site or presence, they must not enter them. This is uninvited intrusion into a family's life, and you and your employer are liable to investigation if you act outside these guidelines. If you have safeguarding/child protection concerns about a child's/young person's behaviour on-line, or if you think a social media platform could provide critical information, for example, if a child is missing or is at risk of harm, the police and children's social care must be contacted. If warranted, the only agency that can access these sites is the police.

School staff will ensure that in private use:

a. No reference should be made in social media to pupils, parents/carers or school staff

b. They do not engage in online discussion on personal matters relating to members of the school community or indeed to any matters relating to school business.

c. Personal opinions should not be attributed to the school or local authority

12. School Website

a. Children's learning will be published on the school website in-accordance with agreement from parents/carers.

b. The website will be edited only by an agreed number of staff which currently includes: DHT, HT, Bursar, Clerical Assistant, Head of Centre and the Learning Support Co-ordinator. All information placed on the website must adhere to the ethos and values of the school's E-Safety Policy.

c. Personal pupil information including home address and contact details will be omitted from school web pages.

d. The school website will not publish the surnames of any pupils.

e. The school will ensure that the image files are appropriately named – and do not use pupils' names in image files if published on the web.

13. Online bullying

Early years children are very unlikely to be victims or perpetrators of online bullying, but their parents/ carers and/or older siblings may be, as may staff and volunteers at the nursery.

Bullying is defined in guidance issued by the Department of Education as: 'behaviour by an individual or group, repeated over time, that intentionally hurts another individual or group either physically or emotionally'[1.]
For further information see our Behaviour Policy.

What is online bullying?

Online bullying is the use of technology, for example mobile phone, email, social networking sites, chat rooms and instant messaging services, to deliberately upset someone else

- It can be used to carry out different types of bullying, as an extension of face-to-face bullying
    - It can also go further as it can invade home/personal space and can involve a greater number of people
- It is an anonymous method by which bullies can torment their victims at any time of day or night
- It can draw bystanders into being accessories
- It includes: threats and intimidation; harassment or 'cyber-stalking'; vilification/defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images (i.e. possible breach of copyright); and manipulation
- It includes sexting - sending explicit images electronically. These images can be subsequently widely distributed
- It also includes trolling; the practice of posting upsetting, provocative, offensive or off-topic messages in an online community. Trolling comments are posted with the deliberate intent of provoking readers into an emotional response, or of otherwise disrupting normal on-topic discussion.

Impact on the victim

The victim may receive email, chat, text messages or posts on social networking sites that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing. Online bullying can pose a serious threat to their physical and emotional safety.

Responding to online bullying

Most cases of online bullying can be dealt with through our behaviour management or safeguarding policies.

In all cases of online bullying make sure that you preserve the evidence.

Some features of online bullying differ from other forms of bullying and may prompt a particular response. For example:

- Change the victim's mobile phone number
- Report the bullying to the site where it was posted
- Try to get content removed from the web
- In some cases, the victim may be able to block the person bullying from their sites and services
- Ask the person bullying to delete the offending content and say who they have sent it on to
- Contact the police in cases of actual/suspected illegal content

What to do if you have concerns about a child / managing allegations against a member of staff

Staff and volunteers should follow the same procedures as for all other safeguarding issues and follow the flow-charts in our Safeguarding Policy.

Conclusion

The school recognises that the use of the internet and ICT devices can substantially and positively impact the quality of teaching and learning of our children and staff. This policy aims to ensure that such use is done safely and appropriately.

Staff/Volunteer/Student Permission Form

Please review the attached school's E-Safety Policy, sign and return this permission form to the Head teacher

School Name: Wentworth Nursery School and Children's Centre

I have read and understood the School's Online-safety policy and will comply with both the ethos and content of the policy. Specifically, I will only use the internet and electronic platforms within an educational context as stipulated within this policy. I will not use any school data, (images, content) on any social media platform, other than those authorised by the Headteacher. Under no circumstances will I discuss school business on any social platform, other than those sanctified by the school.

Name: ……Date……

Signature:……..

Appendix.

Roles and responsibilities

Role	Key responsibilities
Headteacher	• takes overall responsibility for online safety provision • take overall responsibility for data and data security • to ensure the school uses an approved, filtered Internet Service, which adheres to best practice and recommendations • to be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant • to be aware of procedures to be followed in the event of a serious online safety incident. • to receive regular monitoring reports from the Online Safety Co-ordinator • to ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager or IT support company)
Online Safety Co-ordinator / Designated Child Protection Lead	• takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that online safety education is embedded across the curriculum • liaises with school ICT technical staff • To communicate regularly with Leadership Team and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering, and school's change control processes and requests • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • To ensure that an online safety incident log is kept up to date • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: o sharing of personal data o access to illegal / inappropriate materials o inappropriate on-line contact with adults / strangers o potential or actual incidents of grooming o online bullying and use of social media
Governors	• To ensure that the school follows all current online safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub

	Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: o regular review with the E-Safety Co-ordinator / Officer (including: e-safety incident logs, filtering / change control logs)
E-Safety Co-ordinator in relation to curriculum	• To oversee the delivery of the e-safety element in all internet related learning opportunities across the Foundation Stage Curriculum. • To liaise with the Headteacher on curriculum content and internet sites.
Network Manager / Technician	• To report any e-safety related issues that arise, to the e-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack, e.g. keeping virus protection up to date • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • that he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • that the use of the network / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator /Headteacher for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
E-Safety Co-ordinator	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) to the use of ONLY approved sites.
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology; ensure no school business is discussed on social

	platforms. • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Parents/carers	• to support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • to access the school website with the relevant school Acceptable Use Agreement within the e-safety policy • to consult with the school if they have any concerns about their children's use of technology
External group	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school
	•

Glossary of terms

Age related filtering	Differentiated access to online content dependent on age and appropriate need
AUP	Acceptable Use(r) Policy
Blogging & social networking	Anyone can produce and distribute their own content on the internet, and link with other sites to create a very powerful network for sharing ideas and influence opinion
CEOP	Child Exploitation and Online Protection centre (part of the National Crime Agency)
Cyber or online bullying	Bullying using technology such as computers and mobile phones
Downloading	Receiving information or data electronically usually through the internet; this could include saving a document, picture, music or video from a website
Encryption	Computer programme that scrambles data on devices such as laptops and memory sticks in order to make it virtually impossible to recover the original data in event of the loss of the device
E-safety	Limiting risks to children/young people when using Information and Communications Technology (ICT). E-safety is primarily a safeguarding issue not a technological issue, which relates to the use of all ICT: fixed or mobile, current, emerging and future ICT
Filtering	Software that can help to block a lot of inappropriate material but they are not 100% effective
Firewall	A buffer between your computer and the internet. It limits incoming and outgoing information, and keeps your computer safe from intruders. It can't stop you downloading spyware, but it can alert you if a program is sending information over the internet without your permission
Frape	Short for 'Facebook rape', referring to when a Facebook user's identity and profile are compromised and used by a third party to cause upset
Games Console	Examples include XBOX 360, Nintendo Wii, PlayStation, Nintendo DS
Grooming	Online grooming is defined by the UK Home Office as: 'a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'
Hacking	When your details, online accounts or other personal information is accessed by a stranger
ICT	Information and Communications Technology, e.g., mobile phones, gaming consoles, computers, email, social networking
Identity Theft	When your personal information is used by someone else without your knowledge. It may support criminal activity, which could involve fraud or deception

ISP	Internet Service Provider. A company that connects computers to the internet for a fee
Lifestyle website	An online site that covertly advocates particular behaviours and issues pertaining to young and often vulnerable children for example anorexia, self-harm or suicide
Locked down system	In a locked down system almost every website has to be unbarred before it can be used. Only vetted websites can be accessed
Malware	Bad software or programs that damage your computer (viruses), steal your personal information (spyware), display unwanted adverts (adware) or expose your computer to hackers (Trojan horses)
Managed system	In a managed system the organisation has some control over access to websites and ideally offers age-appropriate filtering
Password - strong	A strong password contains a mixture of upper and lower case letters, Numbers and other characters. It is recommended to be a minimum of 8 characters in length
Phishing	Pronounced the same as 'fishing' this is an attempt to trick people into visiting malicious websites by sending emails or other messages which pretend to come from banks or online shops; the e-mails have links in them which take people to fake sites set up to look like the real thing, where passwords and account details can be stolen
Profile	Personal information held by the user on a social networking site
Safer Internet Day	Initiated by the European Commission. Held on the second day of the second week of the second month each year (In 2016 it will be on Tuesday, 9th February)
Sexting	Sending and receiving of personal, sexual images or conversations to another party, usually via mobile phone or instant messaging
SHARP	Example of an anonymous online reporting mechanism (Self Help And Reporting Process)
SNS	Social networking; not the same as computer networking, social networking is a way of using the internet and the web to find and make friends and stay in touch with people
Spam	An e-mail message sent to a large number of people without their consent, usually promoting a product or service (also known as Unsolicited Commercial Email (UCE) or junk email)
Spyware & adware	A general term for malicious software that is designed to take control of a computer without the consent of the user. Adware is one type of spyware: computer programs in which commercial advertisements are automatically shown to the user without their consent
Trojan	A malware program that is not what it seems to be. Trojan horses pretend to be useful programs like word processors but really install spyware or adware or open up a computer to hackers
Trolling	Posting inflammatory messages with the intention of provoking an emotional response
Uploading	Sending and saving information or data from a local system, e.g., mobile phone or computer, to a remote system, e.g., a website
URL	Universal Resource Locator or website address
VOIP	Voice Over Internet Protocol
Youtube	Social networking site where users can upload, publish and share videos. The site is popular, though it has only light moderation and some of its content is of an adult nature