Sheringham Nursery School and Children's Centre

Online and e-safety Policy

Date Approved by the Governing Body: May 2021

Online and E-safety policy

Aim

This policy has been written to ensure children at Sheringham Nursery School and Children's Centre have a safe ICT learning environment. This will be achieved through three main elements:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities.

Roles and Responsibilities

Our e-Safety Co-ordinator is Julian Grenier, headteacher .

All practitioners are responsible for promoting and supporting safe behaviours and following our e-Safety procedures.

All staff should be familiar with our Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social networks;
- Safe use of the school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras; this includes no storage of photos or videos except for hard drives in school and on the cameras. Images must be routinely deleted by class teachers and the Children's Centre co-ordinator.
- Publication of pupil information/photographs and use of website.

Practitioners are reminded / updated about e-Safety matters at least once a year.

How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

Staff must understand the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use, they should discuss this with their line manager to avoid any possible misunderstanding.

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

<u>How will complaints regarding e-Safety be handled?</u>

We will take all reasonable precautions to ensure e-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. We cannot accept liability for material accessed, or any consequences of Internet access.

Staff are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by the Head teacher;
- removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system
- Referral to the local authority and/or police.

Any complaint about staff misuse is referred to the Head teacher.

Complaints related to child protection are dealt with in accordance with our child protection procedures.

Managing the Internet Safely

<u>Technical and Infrastructure</u>

The borough:

- Maintains the filtered broadband connectivity through the London Grid for Learning (LGfL) and so connects to the 'private' National Education Network;

- Ensures their network is 'healthy' by having Local Authority or Synetrix health checks annually on the network;
- Ensures the network manager is up-to-date with LGfL services and policies;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured.

Policy and procedures

At Sheringham Nursery School and Children's Centre, we:

- Supervise children's use at all times;
- Use the pan-London LGfL / Synetrix filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Have additional user-level filtering;
- Preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments;
- Block all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Require all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Make clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings;
- Ensure the named child protection officer has appropriate training;
- Immediately refer any material we suspect is illegal to the appropriate authorities – the Police and the local authority.

Education and training

At Sheringham Nursery School and Children's Centre, we:

- Ensure children and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher
- Teach children a range of skills appropriate to their age and experience:

Managing e-mail

E-mail is now an essential means of communication for staff. Accounts are managed effectively, with up to date account details of users.

- If one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law we contact the police.
- Messages relating to or in support of illegal activities will be reported to the authorities.

- Spam, phishing and virus attachment can make e-mail dangerous. Use filtering software to stop unsuitable mail, LGfL emails reject 9 out of 10 emails received.
- Staff use LA or LGfL e-mail systems for professional purposes;
- Access in school to external personal e-mail accounts may be blocked;
- That e-mail sent to an external organisation is written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style';
    - the sending of attachments should be limited;
    - the sending of chain letters is not permitted;
    - embedding adverts is not allowed;

- Staff sign the appropriate LA / school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Use of Digital and video images

At Sheringham Nursery School and Children's Centre:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is managed by the website manager
- The web site complies with the school's guidelines for publications;
- Most material is our own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number;
- Photographs published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child starts;
- Digital images /video of children are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not use children's names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of children in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- Staff may only use their own cameras in the nursery with the permission of the headteacher, and must use a school memory card.

- Staff may not have their own mobile phones with them whilst in the room with children. These may only be used during a break time in the staff room or other area which is not for children (e.g. not in the crèche, classrooms, or Yellow Room). Photographs of children may not be taken on mobile phones.

Managing Equipment

<u>Using the school network, equipment and data safely</u>

The computer system and network are owned by Sheringham Nursery School and Children's Centre.
We reserve the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely we:

- Ensure staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Make it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Make clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- Have set-up the network with a shared work area for staff. Staff are shown how to save work and access work from these areas;
- Require all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves:
- Request that staff do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day;
- Have set-up the network so that users cannot download executable files / programmes;
- Have blocked access to music download or shopping sites – except those approved for educational purposes;
- Scan all mobile equipment with anti-virus / spyware before it is connected to the network;
- Make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- Make clear that staff accessing LA systems do so in accordance with any Corporate policies
- Do not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  e.g. technical support or SIMS Support through LA systems;
- Provide staff with access to content and resources through the approved Learning Platform which staff and pupils access using their Shibboleth compliant username and password.
- Ensure that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA.
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- Review the school ICT systems regularly with regard to security.

Social media

Social media are any web-based applications, apps etc. which allow users to communicate with each other. They include (this is not an exhaustive list) Facebook, LinkedIn, Tumblr, Instagram, Blogger etc. We recognise that social media play an important part in people's personal and professional lives. But staff must not disclose any information about a child or a family or any other confidential matters, inappropriate information about their work, or otherwise damage Sheringham Nursery School and Children's Centre's reputation by making thoughtless or critical comments on social networking sites. Keeping children safe and acting in their best interests are the key priorities. If in doubt, a member of staff should ask for advice first.

- Staff must not post anything onto social networking sites such as 'Facebook' that could be linked to a child or family, or could be construed to have any impact on our reputation
- Staff must not post anything onto social networking sites that would offend or have a negative impact on any other member of staff or parent. We expect you to use social networks responsibly.
- We advise staff not to allow parents to view your pages, updates etc. on social networking sites. If there is an appropriate reason to allow a connection then staff must ensure that all communication is professional and appropriate at all times. If in doubt, ask for guidance.

How infringements will be handled

Whenever a member of staff infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Head Teacher or senior member of staff deputising.

Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the world wide web that compromises the staff member's professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

Sanction:

- *referred to line manager*

***C*ategory B infringements (Gross Misconduct)**

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school / children's centre name into disrepute.

Sanctions:

- *referred to Headteacher / Governors and follow school disciplinary procedures*
- *report to ITASS/ Human resources*
- *report to Police*

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

The nursery are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child Pornography found

In the case of Child Pornography being found, the member of staff should be **immediately suspended** and the Police should be called: see the free phone number **0808 100 00 40** at: http://www.met.police.uk/childpornography/index.htm

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

http://www.iwf.org.uk

How will staff be informed of these procedures?

- They will be fully explained and included within the school's e-safety / Acceptable Use Policy. All staff will be required to sign the school's e-safety Policy acceptance form;
- The school's e-safety policy will be made publicly available on our website.

Sheringham Nursery School & Children's Centre

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.

(Which is currently: ----------)

- I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Head Teacher.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.

- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location. You must use an encrypted USB or other password-protected system when you need to save files to carry on working on another device (e.g. report writing at home)
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I agree to abide by all the points above.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature

……..Date……

……

Full Name (printed)

Job title

Authorised Signature Head Teacher/senior member of staff deputising

I approve this user to be set-up.

Signature

……..Date……

……

Full Name (printed)