St. Stephen's School
and Children's Centre
Learning for life

Nursery
E-safety Policy

	Date	By	Role	Ratified	Date
Version 1	April 2010	Janet Mantey & Janet Patterson	Deputy head teacher, Assistant head teacher	Governing Body	June 2010
Version 2	May 2012	Janet Mantey	Deputy head teacher	Governing Body	June 2012
Version 3	March 2014	Janet Mantey	Deputy head	Governing Body	March 2014
Version 4	March 2015	Janet Mantey & Duncan Kilty	Deputy Head & IT co-ordinator	Governing Body	March 2015

E-safety Policy

Aim

This policy has been written to ensure children at this nursery 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;
- A comprehensive e-Safety education programme for children, staff and parents.

Roles and Responsibilities

Our e-Safety Co-ordinator is Janet Mantey, the maintained nursery Child Protection Officer is Janet Patterson and the Day Care Child Protection Officer is Julie Haley.

All practitioners are responsible for promoting and supporting safe behaviours in Daycare and follow the settings e-Safety procedures.

All staff should be familiar with the setting's Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- their role in providing e-Safety education for children;

Practitioners are reminded / updated about e-Safety matters at least once a year by the Primary School IT co-ordinator.

We will ensure that efforts are made to engage with parents over e-safety matters and that parents/guardians/carers have signed and returned an e-safety Acceptable User Policy (AUP)form.

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 in nursery, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration will be included in appropriate awareness raising and training. Induction of new staff will include a discussion of the settings e-Safety Policy.

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided once per year.

How will complaints regarding e-Safety be handled?

The nursery 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. Neither the nursery nor the Local Authority can 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/counseling by Manager/Assistant head Teacher/ Head teacher;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system
- Referral to LA / Police.

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

Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Managing the Internet Safely

Technical and Infrastructure

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

The school/nursery:

- Supervises children's use at all times;
- We 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;
- We have additional user-level filtering;
- Staff preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings;

- Ensures the named child protection officer has appropriate training;
- Ensures parents provide consent for pupils to use ICT technologies, as part of the e-safety acceptable use agreement form at time of their daughter's / son's entry to the nursery school;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and training

The nursery:

- Ensures pupils 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:

- Pupils are taught a range of skills appropriate to their age and experience:
- Makes training available annually to staff on the e-safety education program;
- Runs a rolling programme of advice, guidance and training for parents, including:
    - Information leaflets; in nursery newsletters; on the nursery/centre web site
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

Managing e-mail

E-mail is now an essential means of communication for staff in our schools/nursery.

The nursery school:

Does not publish personal e-mail addresses of pupils or staff on the school website. We use *info@st-stephens-pri.newham.sch.uk* for any communication with the wider public.

- 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 may 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

In this school:

- 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 school/daycare web site complies with the school's guidelines for publications;
- Most material is the nursery's 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. Home information or individual e-mail identities will not be published;
- 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 daughter / son joins the nursery school;
- Digital images /video of pupils 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 pupils' 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 pupils 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 not use their own cameras in the nursery.
- 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 whilst in the staff room or off site. 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 / network is owned by the school/nursery.
The school reserves 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 this school: Ensures 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;

- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes 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;
- Has set-up the network with a shared work area for staff. Staff are shown how to save work and access work from these areas;
- Requires 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:
- Requests 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;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes 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.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies
- Does 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; Education Welfare Officers accessing attendance data on specific children
- Provides staff with access to content and resources through the approved Learning Platform which staff and pupils access using their Shibboleth compliant username and password.
- Ensures 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.
- Reviews the school ICT systems regularly with regard to security.

How infringements will be handled

Category A infringements (Misconduct) 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 day care manager/ assistant head teachers/Head teacher.

Staff

- 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:

- *refer to line manager*

Category 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 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 available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Staff can access guidance on e-safety issues on the school's network.