ST NICHOLAS CE (VC) FIRST SCHOOL

E-Safety Policy

March 2015

Contents

Send and Dyslexia Friendly Schools' Policy Statement

At St. Nicholas First School, all pupils are valued equally. Teachers plan lessons which enable all pupils to participate, achieve and excel, whatever their level of ability. Lessons provide opportunities for pupils to recognise and develop their own learning style, (auditory, visual or kinaesthetic), through varied and flexible provision across a broad and balanced curriculum.

In order to meet the needs of all our pupils, we hold the Schools' Dyslexia Friendly, Level 1 Award and are actively working towards Dyslexia Friendly Schools' Full Status.

As a school, we believe that a Dyslexia Friendly environment and teaching styles will benefit the learning of all pupils and not just those with dyslexic tendencies. Strategies that are good for the dyslexic learner are good for everyone.

1. What is E-Safety?

Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young pupils. Some examples of this are:

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

As a school it is our duty of care alongside that of parents and other members of the community to protect our children from these dangers and this can be achieved by many different mechanisms working together.

The purpose of this e-safety policy is to outline what measures the school takes to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

2. Audience

This document is intended for the general public as well as that of school members, parents and local community and is a clear outward statement on the school e-safety practices.

3. General policy statement

The school will endeavour to ensure the e-safety of all school members. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

4. Whole school responsibilities for e-safety

Within the school all members of staff and students are responsible for e-safety, responsibilities for each group include:

Pupils

- Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety lessons

- Reporting any e-safety issue to the teacher, team leader or parent.
- Take responsibility for their own actions using the internet and communications technologies.

- Continuing the good practice taught in school at home.

All Staff

- Have a clear understanding of e-safety issues and the required actions from e-safety training sessions.
- Reporting any e-safety issues to the E-Safety manager as soon as the issue is detected.
- Compliance with a highly visible staff Acceptable Use Policy (AUP) which staff must agree to.
- Maintain security and safety of the school's IT equipment, to protect school data.

Teaching Staff

- Educating pupils on e-safety through specific e-safety training sessions and re-enforcing this training in the day to day use of ICT in the classroom.

Network Manager (Concero)

- Ensure that the best technological solutions are in place to ensure e-safety as well as possible whilst still enabling students to use the internet effectively in their learning.
- Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition securing and preserving evidence of any e-safety breach.
- Checks and audits all systems to ensure that no inappropriate data is stored or is accessible.
- Advises and supports the head teacher in maintaining a robust network

ICT Leader

- Leads the development of the e-safety education programme for students and staff.
- Manages a parental awareness programme for e-safety
- Deals with e-safety breaches from reporting through to resolution in conjunction with the ICT support team and network manager
- Works with the head teacher and school governors to create, review and advise on e- safety and acceptable use policies.
- Works with outside agencies including the police where appropriate.
- Maintains a log of all e-safety issues. ICT

Support Team (Concero)

- Monitors the technology systems which track pupil internet use to detect e- safety breaches.
- Assists in the resolution of e-safety issues with the ICT Leader and other members of staff.

5. How the school ensures e-safety in the classroom

Educating pupils in e-safety

A clear objective of the school is to educate pupils in safe use of ICT and the internet. We feel this is one of the best ways to minimise the potential for any e-safety issues to occur.

- Pupils will receive specific e-safety lessons aimed at ensuring that:
- Pupils know the e-safety risks that exists and how to identify when they are at risk.
- Pupils know how to mitigate against e-safety risks by using e-safe practices whilst online.
- Pupils know when, how and to whom to report instances when their e-safety may have been compromised.
- Pupils know that they are in an environment that encourages them to report e- safety issues without risk of reprimand, humiliation or embarrassment.

The school will follow the Entrust Curriculum Programme by the LEA as one of the primary education tools.

In addition to this specific training all members of staff will have a duty to reinforce e-safety practices wherever possible and will offer students advice and support in the classroom where minor e-safety incidents have occurred. E-Safety practices will be woven into the wider curriculum and reinforced throughout Nursery – Year 4

Acceptable Use Policies

All school members both pupils (as in age appropriate), staff and parents must agree to an Acceptable Use Policy (AUP) before they can use school ICT systems. With respect to e-safety the AUP details:

- The users responsibilities
- Activities which are appropriate and inappropriate
- Best practice guidelines
- How the school will monitor e-safety

- What information is collected

How e-safety is monitored

- The ICT leader will actively monitor the students ICT activity using a monitoring system which can flag potential e-safety issues.
- The ICT leader will periodically review internet access logs to track any websites which could potentially present an e-safety issue.
- The ICT Leader will periodically review the E-Safety log to track and trends and use the information to look at ways of improving the student's e- safety.
- Teaching staff will directly monitor the pupils ICT and internet use in the classroom.

How technology is used

The school will employ many different technologies to help to ensure e-safety for all the school members;

- The school will use internet filtering by RM Technologies to block inappropriate content
- The school will use a system which tracks all student activity on the school's computers. This system will automatically flags potential e-safety issues which will be monitored and then can be investigated by the support for learning team.(PCT)
- The school will restrict which activities the pupils can perform using ICT and the internet through systems security policy and access control.
- Teaching staff will use control mechanisms to attempt to limit the applications and web sites which the pupils can visit whilst using ICT within a lesson.

6. How the School will respond to issues of misuse

The following are provided for the purpose of example only. Whenever a pupil or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Head Teacher.

Pupils:

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: **refer to ICT leader/ HT** / contact with parent/ removal of

Internet access rights for a period]

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to HT / ICT Leader / contact with parent/ removal of Internet access rights for an extended period/ exclusion]

Category C infringements

- Deliberately corrupting or destroying someone’s data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material (Possible Sanctions: referred to HT/ e-safety Manager / contact with parents / removal of equipment/ removal of Internet /exclusion/ referral to police)

Category D infringements

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- 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

(Possible Sanctions – Referred HT /exclusion / removal of equipment / referral to police)

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.
- 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 / Head Teacher / Warning given.]

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school 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 into disrepute.(Sanction – referred to Head Teacher and follow School disciplinary procedures / Police/ Governors / Referral to LADO)

Child Pornography:

In the case of child pornography being found, the member of staff will be immediately suspended and the School disciplinary procedures implemented. The LADO will be contacted.

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 to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.
- Where appropriate, involve external agencies as part of these investigations.

How will staff and students be informed of these procedures?

- Procedures are included within the school's e-safety / Acceptable Use Policy. All staff are required to sign the school's e-safety Policy acceptance form;
- Pupils will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviours'. Pupils are required to sign an age appropriate e-safety / acceptable use form;
- The school's e-safety policy will be made available to parents who are required to sign an acceptance form when their child starts at the school.

7. Working with parents and the community

Clearly many school pupils will also have access to ICT and the internet at home, often without some of the safeguards that are presents within the school environment. Therefore parents must often be extra vigilant about their child's e-safety at home.

One of the goals of the school is to support parent's role in providing an e-safe environment for their children to work in outside the school.

The school will do this in several ways;

- Run training sessions and workshops on e-safety.
- Publish e-safety information and direct parents to external e-safety advisories via the school online parents portal and school website.

8. Acceptable Use Policies

The school has the following acceptable use policies in place which must be agreed to before the relevant individuals will be able to access ICT systems and the internet.

- Staff ICT and the Internet Acceptable Use Policy
- Pupils ICT and the Internet Acceptable Use Policy

A copy of these policies is available on request. The school will regularly review and update these policies.