LANGSTONE ACADEMY

E-Safety Policy

E Safety Policy

This e-safety policy has been developed and shared with;

- Senior Leadership Team (including the Head teacher)
- Teacher with responsibility for computing
- School staff
- Governors

This policy applies to all members of the school communities (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 the schools.

Our schools will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors:

Will require regular updates at meetings to monitor and discuss incident logs, incidents of cyber-bullying, and the provision of e-safety teaching in the school.

Head teacher:

- The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Computing Lead.
- The Head teacher and another member of the Senior Leadership Team / Senior Management Team including Computing Leads should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Teaching, Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e- safety policy and practices
- They have read, understood all relevant policies
- They report any suspected misuse or problem to the Head teacher for investigation /action / sanction
- All digital communications with pupils / parents / carers should be on a professional level

- To closely monitor the use of any digital technology in the school and follow school policy with regard to their use.

- To ensure they are aware of the e-safety curriculum as taught at the School, thereby embedding e-safety into all areas of learning.

Safeguarding Designated Lead & Deputies:

The Safeguarding Lead should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data

- Access to illegal / inappropriate materials

- Inappropriate on-line contact with adults / strangers

- Potential or actual incidents of grooming

- Cyber-bullying

Parents / Carers:

The school will take every opportunity to help parents and carers understand the issues regarding the use of the internet & mobile devices through parents' evenings, newsletters, letters, the school website and information about national / local e-safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events

- Access to parents' sections of the website and on-line pupil records

- Their children's personal devices

Pupils:

The children are responsible for using the school digital technology systems in accordance with the school Technology Use agreement In the Juniors and skills learnt during the teaching of computing in both schools. This is embedded on E safety themed days/weeks across the school year.

Teaching and Learning

Why Internet use is important?

● The Internet is an essential element in 21st century life for education, business and social interaction.

● The school has a duty to provide students with quality Internet access as part of their learning experience.

● Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

● The school Internet access is provided by Schools broadband and monitored by ROCKET. This includes filtering appropriate to the age of pupils.

● An additional filtering set is available in school administration networks only and enables staff access to additional resources.

● Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

● Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation as appropriate to age

● Pupils should be taught based on age appropriateness, to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across it. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

• A planned e-safety curriculum should be provided as part of Computing / PSHE and should be regularly revisited

• Key e-safety messages should be reinforced as part of a planned programme of assemblies (e.g. Safer Internet Day)

• Any request from staff to make accessible sites that would otherwise normally be filtered should be auditable, with clear reasons for the need, and clear educational purpose.

Data Protection Principles will be outlined in a separate Policy.

Social Media Principles will be outlined in the Social Media Policy.

Handling e-safety complaints

● Complaints of Internet misuse will be dealt with by a senior member of staff.

● Any complaint about staff misuse must be referred to the Head teacher using the systems on CPOMs in order to keep clear records.

● Complaints of a child protection nature must be dealt with in accordance with school's safeguarding and child protection procedures or anti-bullying policy if appropriate.

● Pupils and parents will be informed of the procedure.

● Discussions will be held with the Trust and Police as needed to establish procedures for handling potentially illegal issues where appropriate.

Enlisting parents' support

● Parents' and carers attention will be drawn to the school e-Safety Policy in newsletters, on the school website as well via parentmail.

● Parents and carers will from time to time be provided with additional information on e-safety.

Central to the School's anti-bullying policy is the principle that 'bullying is not tolerated' and that the school ethos of 'Care and Respect' and 'Be Excellent Everywhere' is promoted so that 'all pupils have a right not to be bullied'. The school also recognises that it will take note of bullying perpetrated outside school which spills over into the school and so we will respond to any cyberbullying we become aware of carried out by pupils when they are away from the site. Cyberbullying is defined as "an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.”

By cyber-bullying, we mean bullying by electronic media:

• Bullying by texts or messages or calls on mobile phones

• The use of mobile phone cameras to cause distress, fear or humiliation

• Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites

• Using e-mail to message others

• Hijacking/cloning e-mail accounts

• Making threatening, abusive, defamatory or humiliating remarks in on-line forums

Cyber-bullying may be at a level where it is criminal in character. It is unlawful to disseminate defamatory information in any media including internet sites. Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character. The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment. If we become aware of any incidents of cyberbullying, we will need to consider each case individually as to any criminal act that may have been committed. The school will pass on information to the police if it feels that it is appropriate or are required to do so. Parents must ensure that their children are safeguarded from these incidences by not allowing any membership or use of sites that are not legally age appropriate eg. Facebook.

Date: September 2022

Review date: September 2024