Princethorpe Junior School

E- Safety Policy
**Princethorpe Junior School E-Safety Policy**

**Introduction**
The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

At Princethorpe Junior School we want all pupils and staff to be able to make full use of the wonderful digital world, whilst recognising that some material available online may be illegal, upsetting or inappropriate. We seek to teach the pupils how to assess risks themselves in order to help them have a more enjoyable and safer online experience.

This policy applies to all pupils, all teaching staff, all support staff, all governors and all volunteers.

**Aims and Objectives**
It is the aim of Princethorpe Junior School that all pupils will:

- use the internet and other digital technologies to support, extend and enhance their learning;
- develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material;
- develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working;
- use existing, as well as up and coming, technologies safely.

**The role of the Governing Body**

- The governing body will consider and ratify this E-safety policy, and review it annually in the light of guidance from the local authority, or sooner if the local authority issues new guidance in the light of particular circumstances or developments in information and communication technology.
- Governors will consider the evidence of E-safety incident reporting logs when making recommendations for changes to this policy.
- Governors are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that City Council or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children.

**The role of the Head Teacher**

- The Head Teacher is responsible for ensuring that the governing body is offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other school policies, including that on pupils’ behaviour, take account of this E-safety policy.
- The Head Teacher should ensure the school obtains and follows City Council or other reputable guidance on information and communication technology to support this policy.
- The Head Teacher should liaise with a designated senior person to co-ordinate E-safety (Mr Daniel Beier) and ensure that this person has adequate support from, and provides support to, other employees, particularly the designated senior person for safeguarding.
- The Head Teacher will enable the school to provide all employees with training in E-safety relevant to their roles and responsibilities. This training should also be provided to volunteers and school governors who use information and communication technology in their capacity as volunteers or governors, as the case may be.
- The Head Teacher will check that the senior leadership team is aware of the procedures to be followed in the event of a serious E-safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem;
- The Head Teacher will ensure records are kept of all E-safety incidents and that these are reported to the senior leadership team;
The role of the E-safety Coordinator

- The E-safety co-ordinator will oversee the provision of the E-safety curriculum as part of the school’s Computing and PSHE provision to ensure that all pupils are receiving E-safety lessons.
- The E-safety co-ordinator will take day to day responsibility for E-safety issues as well as reviewing the school E-safety policies.
- The E-safety co-ordinator should receive reports of E-safety incidents and create a log of incidents to inform future E-safety developments and act as a record of events in case of further action.

The role of the Teacher and Teaching Assistants

- Teachers must ensure they deliver the E-safety curriculum to their class as dictated by the E-safety co-ordinator.
- Teachers must participate in training in E-safety provided by the school.
- Teachers and teaching assistants should use information and communication technology in accordance with this policy and the training provided.
- Teachers and teaching assistants must report any suspected misuse or problem to the person designated by the school for this purpose.

The role of the Pastoral Care Manager

- If any E-safety incident raises concerns that relate to cyberbullying (see separate policy) or safeguarding then the Pastoral Care Manager will be informed and will take appropriate steps as defined by their role. In the case of safeguarding incidents the DSL will also be notified immediately.

The role of Pupils

- Pupils are expected to use information and communication technology systems and devices as they have been taught and in accordance with the school’s behaviour policy and the instructions given to them by staff.
- Pupils know how and who to report any content or website that they might have intentionally or accidentally accessed which they are concerned about.
- Pupils should immediately report any concern that relates to digital communication, whether on a school device or otherwise, to their nearest trusted adult.

The role of Parents

- Parents who are concerned that their child may be accessing / have accessed inappropriate material either in or outside school should share their concerns with school.
- Parents will be made aware on the Princethorpe Junior School website and possibly by Twitter communication of guidance that is available to help them promote responsible online behaviour outside school.
- Parents have the responsibility to support the school’s e-safety policy and to actively encourage their child to be a responsible digital citizen.

Technical aspects of E-safety

- Princethorpe Junior School will seek to ensure that the information and communication technology systems which it uses are as safe and secure as is reasonably possible by taking reputable advice and guidance on the technical requirements for those systems.
- All staff users who require access to the school network are required to use their unique username and password to access it. The security of their password is their responsibility; should they have any reason to believe it has been compromised they should change it and inform the E-safety co-ordinator.
- Princethorpe Junior School filters internet access for all users, preventing access to illegal content, and with additional filtering for different groups of users for inappropriate content.
- The information and communication technology systems include standard, automated monitoring for illegal materials, profanity, and unsolicited materials (generally known as ‘spam’). This is to safeguard children and adults against inappropriate use.
Monitoring and Review

- This policy is monitored on a day-to-day basis by the Head Teacher who reports to governors about the effectiveness of the policy.
- This E-Safety Policy is the responsibility of the governors and they review its effectiveness annually. They do this by examining the school’s E-safety incidents log (if any have occurred) and by discussion with the Head Teacher and E-Safety Coordinator. Where guidance has been issued by locally or nationally this may take precedence.

Associated Documents

- This policy should be read and applied in conjunction with the behaviour policy, cyberbullying policy, acceptable use policies (staff and pupil) and ICT policy.

Websites offering additional advice and guidance

- Childline
  http://www.childline.org.uk/
- Child Exploitation & Online Protection Centre
  http://www.ceop.gov.uk
- Grid Club and the Cyber Cafe
  http://www.gridclub.com
- Internet Watch Foundation
  http://www.iwf.org.uk/
- Internet Safety Zone
  http://www.internetsafetyzone.com/
- Kidsmart
  http://www.kidsmart.org.uk/
- NSPCC
  http://www.nspcc.org.uk/html/home/needadvice/
- Stop Text Bully
  www.stoptextbully.com
- Think U Know website
  http://www.thinkuknow.co.uk/
- Virtual Global Taskforce – Report Abuse
  http://www.virtualglobaltaskforce.com/

Updated 23.09.17
To be reviewed 23.09.18