E-Safety Policy

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New Internet and online technologies are enhancing communication and the sharing of information. Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- e-mail
- Instant messaging (often using simple web cams) e.g. Instant Messenger)
- Web based voice and video calling (e.g. Skype)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook, Whatsapp)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. YouTube)
- Music and video downloading (e.g. iTunes, Spotify)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access

This policy applies to all members of the school community and should be read alongside the Safeguarding and Child Protection policy

Computing Subject Leader

The computing subject leader will:

- Review the school e-safety policy and practices
- Plan and monitor the computing curriculum, including e-safety
- Provide training and advice for staff
- Provide information for parents/carers

Premises Manager

Premises Manager is responsible for ensuring:

- The school meets recommended technical requirements
- Regular reviews of the safety and security of school technical systems
- Internet access is filtered for all users
- All users have clearly defined access rights to school technical systems and devices
- All users have a username and password

The Premises Manager will liaise with school technical staff

Teaching and Support Staff

The staff are responsible for ensuring:

- 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 and signed the Staff Acceptable Use Policy

- they report any suspected misuse or problem to a member of SLT for investigation
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum
- pupils understand and follow the e-safety responsibilities
- they monitor use of technologies in lessons and other school activities
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that e-safety responsibilities are adhered to in dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Person (DSP)

The DSP 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

Pupils

Pupils:

- are responsible for using the school digital technology systems in accordance with the e-safety responsibilities
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues. 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
- e-safety at home

Parents will be informed that pupils will be provided with supervised Internet access in school, and will be asked to sign and return a consent form for pupil access.

Education – Pupils

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be provided in the following ways:

- a planned e-safety curriculum as part of the computing curriculum
- taking part in events/campaigns e.g. Safer Internet Day

Education – Parents/Carers

The school will seek to provide information to parents/carers through:

- curriculum activities
- the newsletter/web-site
- parents/carers sessions
- high profile events/campaigns e.g. Safer Internet Day
- Reference to relevant web-sites/publications

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should educate pupils about the risks associated with taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet
- Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. These images should not be published on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

- Pupils' full names will not be used anywhere on the school website/newsletter, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/newsletter.

If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the Premises Manager.

Schools will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

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 Headteacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures

Pupil E-Safety Responsibilities

At the start of the academic year children sign an e-safety agreement which covers the following points (modified for children in EYFS and KS1):

- I will ask permission before using the Internet.
- I will only use websites that an adult has approved.
- I will tell an adult if I see anything I am unhappy with.
- I will immediately close any web page I am not sure about.
- I will only e-mail people who an adult has approved.
- I will always send e-mails that are polite and friendly.
- I will not open e-mails sent by anyone I don't know.
- I will never arrange to meet anyone I don't know.
- I will never give out any personal information or passwords.
- I will only use safe chat rooms with adult supervision.

Staff Acceptable Use Policy

ICT and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on ScholarPack) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not browse, download or upload material that could be considered offensive or illegal.
- I will not send to pupils or colleagues material that could be considered offensive or illegal
- Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/ carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..……..…… Date ……

Full Name …….....

Agreed by the Governing Body: **September 2019**
Review Date: **September 2020**
Custodian: **Learning & Achievement Committee**