Scantabout Primary School

Achieving Our Best Together

RATIONALE

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all stakeholders in a child's education from the Head Teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to /loss of /sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video films

- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The E-safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

MONITORING & REVIEW OF POLICY

The implementation of this policy will be monitored and reviewed by the Computing Subject Leader, the Safeguarding Governor and the School's Leadership Team (SLT) at least annually. The Leadership team and the Safeguarding Governor will report to Full Governors on the implementation of this policy at least annually. The E-Safety policy will be reviewed annually, or more frequently in light of any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place. The policy will be monitored through:-

- Logs of reported incidents – recorded on CPOMs;
- Pupil interviews and observations.

SCOPE OF POLICY

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The Education and Inspections Act 2006 and Behaviour and Discipline in Schools 2016, empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

This policy should be read alongside the following school policies:

The Behaviour Policy; Prevent Policy; Safeguarding; Child Protection; Anti-bullying; Staff Acceptable use of ICT and Whistle-blowing.

Roles and Responsibilities

Role	Responsibility
Governors	Monitor the effectiveness of the policy through the Safeguarding Governor; Meet at least termly with the Head Teacher and/or the ICT Subject leader; Monitor the impact of e-safety measures including checking filtering; Carrying out monitoring visits to the school to speak with staff and pupils; Report at least annually to the Full Governing Body on the effectiveness of the policy.
Head Teacher and SLT	The Head Teacher is responsible 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 ICT subject leader; The Head Teacher and SLT are responsible for ensuring that the ICT Subject leader and other relevant staff receive appropriate CPD to enable them to carry out their roles and to train other colleagues as required. The Head Teacher and SLT will ensure that there is a system in place to allow for monitoring and support for those in school who carry out the internal e-safety monitoring role. The SLT will receive regular monitoring reports from the ICT Subject leader. The Head Teacher and other members of the SLT will be aware of the procedures to follow in the event of a serious e-safety allegation being made against a member of staff.
Subject leader	Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school's e-safety policies / documents; Ensures that all members of staff are aware of the procedures to follow in the event of an e-safety incident taking place; Provides training and advice for staff; Liaises with the Local Authority; Liaises with the school's ICT technicians and office staff; Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments; including reporting any filtering issues to HPSN2 Meets regularly with the E-Safety Governor to discuss current issues, review incidents and filtering; Attends relevant meetings, including Full Governors meetings as appropriate; Reports regularly to the SLT.
ICT service provider	Is responsible for ensuring that:

	the school's ICT infrastructure is secure and is not open to misuse or malicious attack; the school meets the e-safety technical requirements outlined in the Hampshire, Isle of Wight, Portsmouth & Southampton 4LSCB E-Safety Strategy http://4lscb.proceduresonline.com/pdfs/esafety_strategy.pdf users can only access the school's networks through properly enforced password protection procedures, in which passwords are regularly changed. the server password is known by authorised personnel only (ICT technician, ICT Subject leader & Head Teacher) Regular backups are undertaken and stored securely HPSN2 is informed of issues relating to the filtering it applies. keeps up to date with e-safety technical information in order to effectively carry out his/her e-safety role and to inform and update others as relevant.
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 and understood and signed the school's Staff Acceptable Use Policy (AUP) at least annually or as required; they report any suspected misuse or problem to the ICT subject leader and/or Headteacher for investigation / action / sanction; digital communications with pupils are on a professional basis only and are only carried out using official school systems; E-safety issues are embedded in all aspects of the curriculum and other school activities; the school's E-safety and Acceptable Use Policy is shared, understood and followed by pupils; pupils have a good understanding of research skills and the need to avoid plagiarism and to uphold copyright regulations; they monitor ICT activity in lessons, extra-curricular and extended school activities; they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices; in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches; their participation in any forum does not breach confidentiality or cause reputational damage to the school (exercise anonymity); their use of ICT does not contravene the General Data Protection Regulation nor breach the school's confidentiality; any documents/equipment/media taken offsite are stored safely and securely, and in accordance with school policy and procedures; report any breaches to the school leadership team, DSL or Data Protection Officer

Designated Safeguarding Lead	Should be trained in e-safety issues and be aware of the potential for serious 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, including potential radicalisation & cyber-bullying.
Pupils	Have a responsibility to: use the school's ICT systems in accordance with the appropriate Pupil Acceptable Use Agreement, which they or their parent will be expected to sign before being given access to school systems; understand the importance of, and the procedures for, reporting incidents of abuse, misuse or access to inappropriate materials; as appropriate follow rules on the use of mobile phones, digital cameras and hand held devices. they should also know and follow school rules on the taking / use of images, and on cyber-bullying. understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school; as appropriate have a good understanding of research skills and the need to avoid plagiarism and to uphold copyright regulations.
Parents/Carers	Parents/Carers play a crucial role in ensuring that their child/ren understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents/carers do not always fully understand the issues and are less experienced in the use of ICT than their child/ren. The school will, therefore, take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and website information about national / local e-safety campaigns / literature. Parents/carers will be responsible for: Endorsing (by signature) the Pupil Acceptable Use Policy; Accessing the school website in accordance with the school's Acceptable Use Agreement.
Community Users	Requests for access to the school's ICT systems by community users will be considered on an individual basis and must be approved by the Head Teacher. Community users will be responsible for: Using the school's ICT systems in accordance with the appropriate Staff ICT Acceptable Use Policy.

Computing within the curriculum

A planned e-safety programme, highlighting key e-safety messages, will be provided as part of ICT and PSHE lessons, and will be regularly revisited; this will cover both the use of ICT and new technologies in school and outside school. Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information. Pupils will be helped to understand the need for the pupil

Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices, both within and outside school.

Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information. They will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Rules for the use of ICT systems and the internet will be posted in classrooms and in the ICT suites.

Members of staff will act as good role models in their use of ICT, the internet and mobile devices. E-Safety will be a focus in all areas of the curriculum and staff will reinforce e-safety messages in the use of ICT across the curriculum. In lessons where internet use is planned, it is best practice that pupils are guided to sites pre-checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Where pupils are allowed to freely search the internet, e.g. using search engines, staff will be vigilant in monitoring the content of the websites visited.

Education and Training Staff

It is essential that staff, according to their role, receive e-safety training and understand their responsibilities as outlined in this policy. Training will be offered as follows:

New staff will receive e-safety briefings as part of their induction programme, ensuring that they fully understand and sign the school's E-Safety Policy and Acceptable Use Policies;

The ICT subject leader will receive external training; regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by the Local Authority and others;

The ICT subject leader will provide advice / guidance / training to individuals as required.

E-Safety training and updates will be delivered to school staff in staff meetings and INSET days. The E-Safety Policy and AUPs will be discussed and signed as part of this training. Further training and updates will be provided at team meetings as appropriate.

Technical Issues

All technical issues are to be reported in writing/via email to the School Office who will contact the IT Systems Administrator for advice/action.

School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Hampshire, Isle of Wight, Portsmouth & Southampton 4LSCB E-Safety Strategy
http://4lscb.proceduresonline.com/pdfs/esafety_strategy.pdf.

All users will have clearly defined access rights to school ICT systems. Users will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames. The administrator passwords are kept securely by the Administration Officer. Users will be responsible for the security of their username and password and must not allow other users to access the system using their log on details, and

must immediately report any suspicion or evidence that there is a breach of security. The school maintains and supports the managed filtering service provided by HPSN2. Any filtering issues must be reported immediately to HPSN2. Requests from staff for sites to be removed from the filtered list will be considered by the ICT Technician and Head Teacher with the Computing subject leader. If the request is agreed, this action will be recorded.

Appropriate security measures will be in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school's systems and data.

Procedures for taking Documents / Equipment / Media Offsite

From time-to-time it may be necessary to take school documents, equipment or media offsite, either for the purpose of working at home or at another location (eg networking with other educational establishments). In such circumstances, staff have a duty to ensure, as far as is possible, the safety and security of the item(s) taken offsite.

The loss of information or equipment, whether containing confidential or sensitive material or not, can seriously damage the reputational standing of the school and may result in disciplinary proceedings being instigated.

The following protocol should be followed:

- documents / equipment / media will not be taken off site without the knowledge and/or permission of the Head Teacher;

- confidential/sensitive items will not be taken offsite without the specific permission of the Head Teacher;

- all items remain the responsibility of the member of staff who has taken them offsite;

- all items will be clearly identifiable as being the property of the school (i.e. labelled with the school name and postcode); confidential/sensitive material will also be clearly labelled and memory sticks encrypted (only the SLT and Administration Officer may use memory sticks in school without the permission of the head teacher); laptops encrypted/password protected (laptops/staff/school passwords must not be shared with anyone other than the IT Technician, the Head Teacher or the Administration Officer);

- During transportation all items will be secured, out of site, in the locked boot of the car. Never leave items unattended in a car. Check your car insurance to ensure that such items are covered for damage or theft.

- Never leave items unattended at home or offsite where they may be susceptible to unauthorised access; Use of school owned equipment/media by family or friends is strictly prohibited;

- Do not store confidential/sensitive items on laptops (this must be kept on site); all child protection and welfare information must be communicated by CPOMs system and not kept on laptops etc;

- Ensure that the screen lock is activated (Control/Alt/Delete) if you have to leave the workstation whilst working offsite;

- Do not retain items offsite unnecessarily - return all items to the school as soon as the work is finished;

- Report any misuse, loss or damage to the Head Teacher immediately.

What to do if you discover or suspect inappropriate use on the web

Follow the procedures outlined in your Acceptable Use Policy agreement. Report all concerns to the Head Teacher/DSL. If your concerns are about the Head Teacher please report this directly to the Chair of Governors or the Local Authority Designated Officer (LADO).

Discovery of indecent material within the school's network is a very serious situation, and must always be reported to the police. It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off. It may be necessary to shut down the whole network, but do not do this unless instructed by the police. Ensure that everyone is kept away and that nothing is touched. Under no circumstances should the E-safety co-ordinator, network manager or Head Teacher attempt to conduct an investigation of their own, or bring in an outside 'expert' to do so, as this may compromise the evidence if a legal case were to result. In some cases this may constitute a criminal offence in itself.

In addition to the police the Head Teacher will also report any concerns to the Children's Services District Manager and the LADO.

In the interests of everyone's professional and personal safety, the following protocol will be followed by all users (staff and pupils):

- never reveal your password to anyone;
- never use the 'remember password' function;
- do not use the same password for systems inside and outside of work;
- do not use any part of your username within the password;
- never write your passwords down or store them where they are open to theft;
- never store your passwords in a computer system without encryption;
- use a 'strong' password (use of symbols and characters);
- change password on a regular basis at least every two terms.

Mobile Phones

Pupils - the school recognises that some parents of older children may wish them to carry a mobile phone so that they can communicate with them before and after the school day. If this is the case, then parents must apply to the Head Teacher in writing and meet with her to agree protocols. In any case, pupils must ensure that they do not use their mobile phone and keep them switched off whilst on site during the school day (8.30 to 4.30).

Staff/volunteer mobile phones are only to be used under the rules stated in the Staff Acceptable Use of ICT Policy. Mobile phones must not be used to store information about pupils or take/store photos of pupils or parents/carers. Mobile phones must not be used in the corridors of the school & pupil areas in the school day. They may be used in the office area or in the staffrooms, unless express permission is given by the Head Teacher.

USE OF DIGITAL IMAGES –PHOTOGRAPHIC / VIDEO

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 or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school staff 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 inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg 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 must not be used for such purposes unless express permission has been given by the Head Teacher for one off exceptional circumstances. In such cases, the member of staff will ensure that all images are deleted from their personal camera after use and will confirm this with the Head Teacher.

• Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

• Pupils must not take, use, share, publish or distribute images of others without their permission

• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

• Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Data Protection

The school and staff will ensure that data which is recorded, processed and stored by the school and its staff are fully compliant with the General Data Protection Regulations (2018).

Formulated June 2018;

Next review: Summer 2019