E-Safety Policy

Heckington St. Andrew's Church of England Primary School

Approved by:	Jonathan Powell	**Date:**	May 2019
Last reviewed on:			
Next review due by:	May 2020		

Rationale & Scope of this policy

National guidance suggests that it is essential for schools to take a leading role in e-safety. BECTA (British Educational Communications & Technology Agency) in its "Safeguarding Children in a Digital World" suggested:

"That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, BECTA recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school.

Recognising the growing trend for home-school links and extended school activities, BECTA recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT too."

The Education and Inspections Act 2006 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.

Roles and Responsibilities

Governors: Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

Head teacher and senior leadership team: The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community. The Head teacher / Senior Leaders are responsible for ensuring that the relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant. The Head teacher and another member of the Senior Leadership Team 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 (see Whistleblowing Policy.).

Computing subject leader: Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents and ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place. They also provides training and advice for all staff and liaise with the Local Authority where applicable. As subject leader they should also receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments and where required liaise with ARK to adjust the schools internet filtering.

Teaching and Support Staff: Teaching and 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 and that they report any suspected misuse or problem to the Computing subject leader / Head teacher / Senior Leader for investigation / action / sanction. All digital communications with pupils (email / Virtual Learning Environment (VLE) should be on a professional level and only carried out using official school systems. When teaching e-safety issues should be embedded in all aspects of the curriculum and other school activities and pupils should

understand and follow the school e-safety code of conduct for acceptable use. Pupils should also have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations where appropriate. In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that E-Safety processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils: Are responsible for using the school ICT systems in accordance with the code of conduct which all pupils sign each half term.

E-Safety Education

Pupils E-Safety education will be provided in the following ways:

- In accordance with the 2014 National Curriculum requirements, planned e-safety teaching will be provided as part of Computing / PHSE /other curriculum areas (as relevant) and should be revisited at the beginning of every half term – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of any lesson in which pupils are using technology.
- Pupils will all sign a key stage specific code of conduct each half term
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Filtering

Filtering is provided and administered by ARK. Any filtering issues should be reported immediately to the computing subject leader or

to the head teacher / senior leadership. Any requests from staff for sites to be removed from the filtered list will be forwarded to ARK in consultation with the computing subject leader, the head teacher or a member of the senior leadership team.

Use of digital and video images

When using images and video, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. It is vital both staff and pupils are aware of and take responsibility for their digital footprint. 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 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 e.g. 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, under no circumstances should the personal equipment of staff be used for such purposes. Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the school's home school agreement (which seeks parental consent) on the use of

images and the school's GDPR policy. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Communication technologies

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the Head teacher or senior leadership in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at Foundation Stage / KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate

emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Data protection

We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018. Staff will ensure they properly log-off from a computer terminal after accessing personal data. Staff will not remove personal or sensitive data from the school premises without permission of the head teacher. Any data which is impractical to ensure is kept in school (eg Reports) will be kept secure, by use of encrypted memory sticks which are password protected.

Acceptable Use Policy

Use of the Internet is now an integral part of people's lives. In spite of this, it is important schools continue to be aware of issues and problems and to continue to educate our children accordingly. It is important staff, pupils and parents understand the moral and ethical issues surrounding access to the Internet before allowing access.

There are a number of options available that restrict access to the Internet, but it must be understood that no system, other than a ban on using the Internet, can ensure users do not access material that is deemed inappropriate.

Pornographic material is usually the main focus of filtering methods, but users need to be aware that removing racist, sexist and political

material is beyond many filtering programs. There is also the difficulty with any filtering software that content which is deemed offensive to one group of people is regarded differently by others. Furthermore, we are now faced with more recent issues such as grooming, cyber-bullying and identity theft which cannot be controlled by filtering systems. For these reasons, treating the use of the Internet as an issue that involves pupils, staff and parents has to be the most sensible approach.

In response to this, the Heckington St Andrews school has an Acceptable Use Policy, together with rules for safe internet use. These rules are a joint agreement between staff and pupils as part of our ESafety curriculum. The policy is available to parents on request and electronically via our website.

Today millions of people use the Internet and e-mail on a daily basis. In recent years, use of the Internet has continued to increase, particularly with the introduction of mobile devices. This is not only for business and personal use, but also for educational purposes. A wealth of educational resources is now available on the Internet and via mobile devices; and this continues to grow. At Heckington St Andrews Primary School, we believe that our pupils should have opportunity to use these emerging and changing technologies to support their learning and to equip themselves with the skills that will be required for lifelong learning. Resources found on the Internet, are unlike those found in more traditional media. Historically, resources such as books, videos and other resources could be carefully selected for the learning process. The Internet, by its open and dynamic nature, may lead pupils to material over which the teacher has had no previous viewing and has therefore been unable to judge its suitability for classroom use. Although the school will endeavour to point pupils to relevant curriculum sites or

to previously researched sites that have been identified as being relevant to the area of study, we also accept our responsibility in educating our pupils about responsible, respectful and safe use of the Internet.

Research using electronic methods is now fundamental to preparing pupils for citizenship and future employment possibilities. The school will ensure that opportunities for both integrating the use of the Internet into the curriculum and teaching pupils about e-safety will be planned and that staff will guide pupils in line with Government guidelines. Staff will be given regular opportunities to discuss issues surrounding the use of the Internet and e safety and develop appropriate teaching strategies. In addition, relevant governmental guidelines will be made available to all staff as a point of reference. The school uses an Internet Service Provider (ISP) that has filtering software in place to minimise the risk of accessing inappropriate Internet material or receiving inappropriate e-mail. Should any pupils access material they have concerns about, they should notify a member of staff, who will then inform the Computing subject leader, head teacher or member of senior leadership. Where possible, appropriate action will then be taken to block further access. On occasions where a total block is not possible, staff will then use this to remind pupils of their own responsibilities in becoming safe users, in line with the Computing curriculum. The school will take appropriate action against users that use the school facilities to knowingly access, or attempt to access inappropriate materials. Therefore, the school reserves the right to access the work area of any user to view files held in that area.

All pupils across the school have access to the Internet and are able to use the technology available. It is anticipated that access to younger pupils will be more directed, with autonomous use being

available to older pupils. Where pupils are given freedom to search the Internet for information, they should be given clear learning objectives by their teacher. In the event of inappropriate use or the accessing of inappropriate materials, action will be taken by the teacher, computing subject leader, senior leadership or the Head. Any incidents will be reported and logged by computing subject leader and where appropriate a member of the child protection team. Pupils will be taught to use e-mail, the Internet and mobile technology responsibly to reduce the risk to themselves and others. After being agreed by staff and pupils at the beginning of each half term, the code of conduct for Internet access and the use of all technologies within school will be signed by each pupil and posted in each classroom. E safety will form an integral part of Computing lessons.

The school believes that access to the Internet and mobile devices will enable pupils to explore resources available from libraries, other schools, LAs and commercial content providers in a way that will enhance the learning process in ways impossible by other means. E-mail will allow communication to be made with other individuals and organisations, regardless of time and distance. The school believes that access to this technology brings benefits to the learning processes that outweigh the possible risks that might be encountered.

Heckington St Andrew's
Church of England
Primary School

E-SAFETY CODE OF CONDUCT Foundation Stage, Years 1 & 2

You should:

- ☺ ALWAYS follow the instructions of your teacher.
- ☺ ALWAYS be nice and polite when you send messages to other users.
- ☺ ALWAYS tell your teacher if you see, hear or read anything which makes you feel uncomfortable while using the computer.
- ☺ ALWAYS use your own log in.

You should:

- ☹ NEVER send anyone a message which is not nice.
- ☹ NEVER use bad or annoying language.
- ☹ NEVER tell a stranger any of the following information:
- your name
- your home address
- your telephone numbers
- any other personal information about yourself or any of your friends.

When you are finished using a computer / iPad you should always close it down properly following your teacher's instructions.

I agree to follow our code of conduct signed:

Heckington St Andrew's
Church of England
Primary School

E-SAFETY CODE OF CONDUCT Years 3, 4, 5 & 6

You should:

- ☺ ALWAYS follow the instructions of your teacher who will guide you towards appropriate sites.
- ☺ This also applies during 'My Time'.
- ☺ ALWAYS be aware that your actions on the Internet can be seen by others.
- ☺ ALWAYS be nice and polite when you send messages to other users.
- ☺ ALWAYS tell your teacher if you see, hear or read anything which makes you feel uncomfortable whilst using the Internet.
- ☺ ALWAYS use your own log in.
- ☺ ALWAYS respect copyright and trademarks. You cannot use the words or pictures that you see on an Internet site without giving credit to the person that produced the information originally. You must not copy text or pictures from the internet and hand it in to your teacher as your own work.
- ☺ ALWAYS check with a Teacher before downloading files, completing questionnaires or opening email attachments

You should:

- ☹ NEVER send, access, store or display any nasty messages or pictures.
- ☹ NEVER use or send bad, threatening or annoying language.

☹ NEVER access anybody else's work or email

☹ NEVER intentionally waste resources e.g. printing without permission

☹ NEVER tell a stranger any of the following information:

- your name
- your home address
- your telephone numbers
- any other personal information about yourself or any of your friends.

When you are finished using a computer / iPad you should always close it down properly following your teacher's instructions. Failure to follow the code will result in loss of access and further disciplinary action may be taken if appropriate. If applicable, external agencies may be involved: certain activities may constitute a criminal offence.

I agree to follow our code of conduct signed: