SAPIENTIA EDUCATION TRUST

Great Hockham Primary School and Nursery

E-safety including acceptable use Policy at GHPS & N

Author / Edited by	Claire Fowler
Date	July 2021
Review Body	Local Governing Body
Review frequency & next review due	As required

SAPIENTIA EDUCATION TRUST

Great Hockham Primary School and Nursery
School E-Safety & Acceptable Use Policy

Background / 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. The development and implementation of such a strategy involves all the 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 files
- 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 (e.g. behaviour, anti-bullying, remote learning, safeguarding and child protection 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.

Scope of the 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 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students / 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.

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- Key e-safety messages should be reinforced as part of a planned programme of assemblies/pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Pupils should be helped to understand the need to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Rules for use of ICT systems / Internet will be posted in the ICT suite
- Staff should act as good role models in their use of ICT, the Internet and mobile devices

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented

School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance. The filtering system used is Senso and the headteacher has a login to this site

There will be regular reviews and audits of the safety and security of school ICT systems. Servers, wireless systems and cabling must be securely located and physical access restricted. All users will have clearly defined access rights to school ICT systems and all users will be provided with a username and password

Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security

Appropriate security measures are present to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum

In lessons where internet use is pre-planned, it is best practice that 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

Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
Pupils should 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.

Use of digital and video 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 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; the personal equipment of staff should not be used for such purposes.

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 students / pupils will be selected carefully and will comply with GDPR with regards the use of such images

Students' / 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

Pupil's work can only be published with the permission of the pupil and parents or carers

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

The official school email service is regarded as safe and secure and is monitored

Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems

Users need to be aware that email communications may be monitored

Users must immediately report 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 pupils or parents / carers

(email, chat, VLE etc) must be professional in tone and content

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

Staff must ensure that they:

At all times take care to ensure the safe keeping of personal data, minimising the risk its loss or misuse

Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they using personal data

Unsuitable / inappropriate activities

Some Internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. In addition, the school also bans the use of school systems for the following:

Pornography
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
Using school systems to run a private business
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and

passwords)
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
On-line gaming (non educational)
On-line gambling
On-line shopping / commerce
File sharing with people other than approved agencies

Mobile phone communication and instant messaging

No children are allowed mobile phones in school

- If a child requires a mobile phone before or after school the child may take the phone to the office to be securely locked away until the end of the school day.
- Staff are not to give their home telephone number or their mobile phone number to pupils.
- Staff are not to make use of pupils' mobile phone numbers either to make or receive phone calls or to send to or receive from pupils' text messages.
- Photographs and videos of pupils should not be taken with mobile phones, other than in exceptional circumstances and with the knowledge and permission of a member of the SLT.
- Staff should not enter into instant messaging communications with pupils.
- Mobile phone communication should be used sparingly and only when necessary, children should not be present unless necessary. All staff are encouraged to leave mobile phones, switched off in their bags which should be left in a classroom cupboard or other safe place during lesson times. If staff expect to receive a call during lessons time they should direct the caller to the school landline in the office.

The school permits the use of personal mobile phones on trips to contact the school if/when appropriate and necessary.

SAPIENTIA EDUCATION TRUST

Appendix A

Internet Safety and the use of Social Media – Year 5 & 6

Dear Parent/Carer

Internet safety and the use of Social Media – Year 5 and 6

Great Hockham Primary School and Nursery is committed to promoting the safe and responsible use of the internet and as such we feel it is our responsibility to raise this particular issue, due to the increase in inappropriate use of Skype, Snapchat, Instagram, Facebook and group games. Many of the issues that have been brought to our attention recently have involved the use of:

Skype - a video and messaging app. You are required to be at least 13 years old before you can create an account

Tik-Tok – a social networking site which allows users to create and share short videos. The recommended age for this site is 13+ years

Snapchat - a photo and video sharing app allowing images and texts to be sent and automatically deleted after a set amount of time. You are required to be at least 13 years old before you can create an account

Instagram - an online mobile photo sharing, video sharing and social networking service which enables its users to take pictures and videos and share them on a variety of social networking platforms. You are required to be at least 13 years old before you can create an account

Facebook - a social networking site. You are required to be at least 13 years old before you can create an account

WhatsApp – An instant messaging app for smartphones. The user agreement requires users to be age 16 or older. Children are often creating ‘groups’ to which others are joining. This means that all information is shared with anyone who is in the group so privacy is lost and in some cases strangers have been added to the group

Fortnight - a group game where children can be muted and excluded from groups. The recommended age for this game is 13 years

We understand that it is increasingly difficult to keep up with the ways that our children are using new and ever changing technologies. Our children are immersed in a society that has become dependent on powerful computers, including smart phones, iPads, interactive online games and virtual communities.

Websites such as Facebook, Instagram, Skype and WhatsApp to name but a few, offer fantastic opportunities for communication and social connections, however they are created with their audience in mind especially sites such as Facebook and Instagram which are specifically for those over 13 years old. When monitoring your son/daughter's internet use, please remind yourself of the concerns of social media:

Many sites use 'targeted' advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated when they registered. They may have lied about their age to get an account, making them appear older than they are, increasing this risk.

• Young people may accept friend requests from people they don't know in real life which could increase the risk of inappropriate contact or behaviour. The general rule is, if they aren't friends in real life, they shouldn't be 'friends' online

• Language, games, groups and content posted or shared on social media is NOT moderated, and therefore can be offensive, illegal or unsuitable for young people

• Photographs shared by users are NOT moderated and therefore young people could be exposed to inappropriate images or even post their own

• Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and options

• Social media sites can be exploited by bullies and for inappropriate contact

• Social media sites cannot and do not verify its members, therefore, it is important to remember that if your son/daughter can lie about who they are online, so can anyone else

Primarily, these occurrences and reported incidents of misuse of social media sites happen at home, after school hours when children have access to web sites that are blocked in school. With this in mind, and in response to concerned parents who have asked for advice regarding internet safety, we feel it important to point out to parents the risks of unregulated use of such sites, so you can make informed decisions as to whether to allow your child to have a profile or not and when and how to monitor their use, particularly at night time. We strongly advise a device free bedroom policy

after bedtime to allow for uninterrupted sleep and rest.

Although we cannot govern matters occurring out of school hours which is parental responsibility, we will take action (such as reporting under age profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our pupils, including reporting the use of inappropriate images of young people to the police, as this is a legal matter. This also refers to inappropriate text messages.

Should you decide to allow your child to have an online profile we strongly advise you:

• Check their profile is set to private and that only their friends can see information they post

• Monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting or messaging offensive /inappropriate messages or photo's

• Monitor your child's use of language and how they communicate to other people, ensuring profanity is discouraged

• Have a look at advice for parents on the social media sites

• Set up your own profiles so you understand how the site works and ask them to have you as their friend on their profile so you know what they are posting online

Make sure your son/daughter understand the following rules:

- Always keep your profile private
- Never accept friend you do not know in real life
- Never post anything which could reveal your identity including photographs wearing school uniform where possible
- Never post anything you wouldn't want your parents or teachers to see
- Never agree to meet somebody you only know online without telling a trusted adult
- Always tell someone if you feel threatened or someone upsets you

We recommend that all parents visit the CEOP Think U Know website for more information on keeping your child safe online and also use the information we send home on how to keep your child safe. The school website has pages for parents and for children dedicated to keeping safe online.

Through lessons provided at school, assemblies, guest speakers, and PSHE lessons, we do our best to provide our children with the awareness and knowledge they need in order to recognise and avoid dangerous, destructive, or unlawful behaviour and to respond appropriately. However, it is only through a collaborative effort between parents and teachers that we will succeed in creating responsible and safe cyber citizens. Our website provides links to other sites that can provide lots of advice and support.

The school's internet and network is managed by Sapientia Education Trust and has the highest levels of cyber security to help keep your child safe. Children receive regular lessons and assemblies on how to keep safe online and who to talk to if they are worried. They are also taught how to publish online responsibly and safely and how to evaluate content in terms of reliability.

Children sign an acceptable use of the internet agreement annually which is explained to them at an appropriate level.

The school seeks permission from parents to post photographs of their children on its website and there is a 'no mobile phone use in school' policy.

All staff have anonymised online presence and are forbidden from befriending pupils online. Given the close nature of our community, it is acknowledged that most staff will inevitably have friends who are also parents; with this in mind, all staff are reminded that they need to be aware of this fact when using social media.

If you require any further advice or information, please do not hesitate to contact us at the school.

Appendix B:

Great Hockham Primary School's Staff, Governor and Student Acceptable Use Agreement / ICT Code of Conduct

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

- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras; email, social networking and that ICT use may also include personal ICT devices when used for school business.

- I understand that it is an offence to use a school ICT system and equipment for any purpose not permitted by its owner.

- I will only use the school's email / Internet / Public space and any related technologies for uses permitted by the Head 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 understand that I am responsible for all activity carried out under my username

- I will ensure that all school generated electronic communications are appropriate and compatible with my role.

- I will only use the approved, secure email system(s) for any school business

- I will ensure that all data is kept secure and is used appropriately and as authorised by the Head teacher or Governing Body. If in doubt I will seek clarification. This includes taking data off site.

- At school, I will not install any hardware or software without the permission the head teacher.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images will only be taken, stored and used for purposes in line with school policy and with written consent of the parent, carer or adult subject. Images will not be distributed outside the school network/learning platform without the consent of the subject or of the parent/carer, and the permission of the Head teacher.

- I understand that my permitted 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 Head teacher.

- I will respect copyright and intellectual property rights.

- I will not jeopardise the safety or wellbeing of any child or adult in the school through my use of ICT.

- I will report any incidents of concern regarding children's safety to the Senior Designated Professional or Head teacher.

- I will have an anonymised online presence for social media use

User Signature

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

Full name ..... (printed)

Role:……..…

Signature:……**Date:**……

Appendix C:

Great Hockham Primary School's E-safety agreement form for parents and carers

Parent / guardian name:*……..*

Pupil name: …….

Pupil's class: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet and other ICT facilities at school.

I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use and understand that my son/daughter may be informed if the rules have to be changed during the year. I know that the latest copy of the E-Safety Policy is available from the school office or on the school website and that further advice about safe use of the Internet can be found on the school's website.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service; employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent's signature:…… **Date:**…….

Appendix D:

Great Hockham Primary School's E-safety Rules (Key Stage 2)

These E-safety Rules help to protect students and the school by describing acceptabl computer use.

- I will ask permission before using the internet or school network at school.
- I understand the school owns the computer network and can set rules for its use to keep me safe.
- I will only use ICT systems in school, including the internet, email and digital pictures for school purposes.
- I will only log on with my own user name and password.
- I will not share my passwords with anyone.
- I will make sure that all messages are responsible, respectful and sensible.
- I will be responsible for my behaviour when using the Internet/learning platform. This includes resources and the language I use.
- I will not give out any personal information about myself or anyone else when using the internet.
- If I accidentally come across any material that makes me uncomfortable I will report it to a teacher.
- I will not download or install software.
- I will respect the privacy and ownership of others' work on-line at all times.
- I understand the school may watch my use of the school's computer systems and learning platform.
- I understand that I will only be allowed to use the school equipment and systems by following these rules.

Pupil name: ……

Pupil signature: …… **Date:**……

Great Hockham Primary School's E-safety Rules (Key Stage 1)

- I will only use the internet when an adult has given me permission.
- I will only click on the buttons or links when I know what they do.
- I will only search the Internet when an adult is in the same room.
- I will always ask if I get lost on the Internet
- I will ask or tell an adult straight away if I am unsure of something.
- I know that the school will watch what I'm doing to keep me safe.
- I will not share anything personal about myself e.g. my name or address.
- I agree that I will follow these rules when using any electronic device at school.

Pupil name: ……

Pupil signature: …… **Date:**……

Great Hockham Primary School's E-safety Rules (Foundation Stage)

- I will always ask an adult before using the computers.
- I will only use the programs and internet sites I have been shown how to use.
- I will remember the rules by Smartie and not click on anything if I don't know what it is.
- I will tell an adult straight away if something unusual happens or I feel uncomfortable.
- I know that the school will watch what I'm doing to keep me safe.
- I agree that I will follow these rules when using any electronic device at school.

Pupil name: ……

Adult signature to confirm these were read to and understood by the child: ……

Date:…….

Appendix E:

Great Hockham Primary School
Use of digital images - photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

- Where showcasing examples of pupils work we only use their first names, rather than their full names.
- If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.
- Only images of pupils in suitable dress are used.
- Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- **Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity; e.g. photographing children at work and then sharing the pictures on the interactive whiteboard or the visualiser in the classroom allowing the children to see their work and make improvements.**
- **Your child's image for presentation purposes around the school; e.g. in school wall displays, presentations and the website to capture images around the school or in the local area as part of a project or lesson.**
- **Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators; e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus, school website or local newspaper/magazine. In rare events, your child's image could appear in the media if a newspaper photographer or television film crew attend an event.**

Note: If we, or you, actually wanted your child's image linked to their full name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Use of digital images - photography and video:

I agree to the school using photographs of my child or including them in video

material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Name of Child:_____

Parent / guardian signature:_____ **Date:**___/___/___