Date: June 2016

Gilthill Primary School

E- Safety Policy

E- Safety Policy

Policy development

The e-safety policy is part of the School Development Plan and relates to other policies including those for ICT, Anti-bullying and Safeguarding children.

- Our policy has been written with full consultation from staff in school, parents/carers, governors and young people.
- It has been agreed by senior managers and approved by governors
- The policy and its implementation will be reviewed annually
- It is available to read or download on our school website or as a hard copy from the school office

Roles and responsibilities

The school has an e-safety coordinator (in some cases this will be the Designated Safeguarding Lead as the roles may overlap). Our coordinator is: Mrs S Lamb and Mrs S Cregan

Teaching and Learning

Why internet and digital communications are important

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and be given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact. This will include using the CEOP icon or the Hector Protector function.
- Issues such as Cyberbullying and e-safety will be built into the curriculum to encourage self – efficacy and resilience. Some children who have had problems or with additional needs may need additional support.

Managing Internet Access

Information security system

- The school ICT system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies may be discussed with the Local Authority

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system Pupils must immediately tell a member of staff if they receive offensive e-mail.
- Staff to pupil e-mail communication must only take place via a school e-mail address or from within a learning platform and will be monitored
- All incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the school's website should be the school address. No staff or pupil's personal details will be published
- The headteacher or their nominee will have overall editorial responsibility to ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include children will be selected carefully and will not enable individuals to be clearly identified. Group photographs will be used rather than full-face photos of individual children.
- Pupil's full names will be avoided on the website and learning platforms including blogs, forums especially if associated with a photograph.
- Written permission will be obtained from parents and carers before any photographs are published on the school website
- Parents should be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites and consider how to educate pupils in their safe use. This may not mean blocking every site; it may need monitoring and educating students in their use
- The school will encourage parents to support their children when setting up a social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites.
- Pupils will be advised never to give out personal details which may identify them or their location.

Managing filtering

- The school will work with the County Council or their own Academy group to ensure systems to protect pupils are reviewed and improved.
- Any unsuitable on-line material should be reported to the e-safety coordinator
- Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.
- A log will be kept and used to identify patterns and behaviours and therefore inform policy and educational interventions.

Managing video conferencing

- Video conferencing will be appropriately supervised for the pupils' age.
- Pupils will always ask permission from the supervising teacher before making or receiving a video conference call.
- Video conferencing will use the educational broadband network to ensure quality of service and security.

Managing emerging technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones and associated cameras will not be used in lessons or formal school time except as part of an educational activity.
- Care will be taken with the use of hand held technologies in school which may not have the level of filtering required.
- Staff will use a school phone where contact with pupils and their families are required.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

Policy decisions

Authorising internet access

- All staff must read and sign the 'staff code of conduct before using any school ICT resource
- The school will maintain a current record of all staff and pupils who are given access to school IT systems
- Parents will be asked to sign and return a consent form
- At Key stage 1, access to the internet will be by adult demonstration with directly supervised access to specific on-line materials.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material; however it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor ICT use to establish if the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Complaints of misuse by staff will be referred to the headteacher
- Any complaints of a child protection nature must be dealt with in accordance to child protection procedures.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with the schools behaviour policy.

Community use of the internet

- All use of the school internet connection by community and other organisations shall be in accordance with the e-safety policy.

Communicating the policy

Pupils

- Appropriate elements of the e-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms
- Pupils will be informed that network and internet use will be monitored.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified,

Staff

- All staff will be given a copy of the e-safety policy and required to sign to acknowledge that they have read and understood the policy and agree to work within the guidelines.
- Staff should be aware that the system is monitored and that professional standards are expected.
- Staff monitoring the system will be supervised by senior management and have a clear procedure for reporting

Parents

- Parents will be notified of the policy in newsletters, the school brochure and website
- All parents will be asked to sign the parent/pupil agreement when they register their children.
- Parents will be offered e-safety training to encourage them to support and encourage positive online activities with their children and help them to use the internet safely.

This E-safety policy was revised by: Mrs S Lamb

On (date): April 2016

It was approved by the Governors on: May 2016

E-safety Agreements and Rules

E-safety rules for Key stage 1

Think then Click

These rules help us to stay safe on the Internet

I only use the internet when an adult is with me.

I can click on the buttons or links when I know what they do.

I can search within websites chosen by an adult.

I always ask if I get lost on the Internet.

I can send and open emails with adult help.

I can write polite and friendly emails to people that I know.

E-safety rules for Key stage 2

Think then Click

- I only use the Internet if I have permission.
- I will only use websites that an adult has chosen
- I will tell an adult if I see anything I am uncomfortable with.
- I will only e-mail people an adult has approved.
- I will send and post messages and comments that are polite and friendly.
- I will never give out passwords or personal information.
- I will not open e-mails sent by anyone I don't know.
- I will not use Internet chat rooms.
- I will never arrange to meet anyone new that I have only chatted with on-line.

Staff, Governor and Visitor Template Acceptable Use Policy/ICT Code of Conduct Gilthill Primary

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our working life in school. This policy is designed to ensure 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.

- I appreciate that ICT includes a wide range of systems and devices including mobile phones, PDAs, digital cameras, email, social networking and may include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- 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 activities carried out under my user name.
- I will only use the school email, internet, intranet, Learning platform or any related technologies for professional purposes.
- I will ensure that personal data is kept secure and used appropriately, whether in school, taken out of school or used remotely when authorised by the headteacher or governing body.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will respect copyright and intellectual property rights.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without permission.
- I will ensure that my online activity both in school and outside school will not bring my professional role into disrepute.
- I will ensure that all electronic communications with parents, pupils and staff are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school's e-safety policy and help pupils to be safe.
- I will report any incidents of concern regarding children's safety to the e-safety coordinator, the Child Protection Officer or the head teacher
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

User Signature

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

Full Name: _____

Job Title: _____

Signature_____ Date_____

Parent/Carers consent form and e-safety rules

All pupils will have access to the school's computer facilities including the internet as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-safety rules have been understood and agreed.

Pupils Name: _____

Parent/Carer Name: _____

- As the parent or legal guardian of the above pupil, I have read and understood the attached school rules and now grant permission for my son/daughter to use the internet, school e-mail system, learning platform and other ICT facilities at School.
- I know that my son/daughter has signed an e-safety agreement and they have a copy of the school e-safety rules.
- We have discussed this document and they agree to follow the rules to support the safe and responsible use of ICT at School.
- I accept that the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that they will take every reasonable precaution to keep pupils safe and to prevent pupils accessing inappropriate materials.
- The school has an educationally filtered service, restricted access email and provides age appropriate teaching around internet use and e-safety issues.
- 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.

Parents Signature: _____ Date: _____

Please complete and return to the school office.

This page has been left blank intentionally

Use of Children's Images/Photographs

Gilthill Primary School believes that the responsible use of children's images can make a valuable contribution to the life and morale of the school. The use of photographs in school publicity materials can increase pupil motivation and help parents and the local community identify and celebrate the school's achievements.

We only use images that the Headteacher and Governing Body consider suitable and which appropriately represent the range of activities the school provides and the values it adheres to. No images will be used which could be considered to put any child at increased risk.

Through this policy we aim to respect young people's and parents' rights of privacy and minimise the risks to which young people can be exposed through the misuse of images. The policy takes account of both data protection and child protection issues.

Data protection

Photographs and video images of pupils and staff are classed as personal data under the terms of the Data Protection Act 1998. We will not use images of identifiable individuals for school publicity purposes without the consent of either the individual themselves or, in the case of pupils, their parent, guardian or carer.

In seeking consent we will ensure that parents are clear why we are using a child's image, what we are using it for, and who might want to look at the pictures. Our consent form makes clear the period of time for which consent applies.

All images will be stored securely and used only by those who are authorised to do so.

Child protection

We will only use images of children in suitable dress. The Headteacher and Governing Body will decide if images of some activities – such as sports or arts – are suitable without presenting risk of potential misuse.

Any evidence of the use of inappropriate images, or the misuse of images, will be reported to the school's child protection designated teacher, the LA, Social Services and/or the police as appropriate.

We will use first names only in conjunction with an image and we will never use an image of a child who is subject to a court order.

Websites

We will adopt the same principles as outlined above when publishing images on the internet as we would for any other kind of publication or publicity material. However, the school recognises that there is no control over who may view images, and consequently a greater risk of misuse of images, via the internet. We will therefore give specific consideration to the suitability of images for use on the school's website.

Images, and accompanying details, will only be used in line with government guidance as outlined on the Department for Education and Skills Superhighway Safety website (http://safety.ngfl.gov.uk/schools/).

Webcams and mobile phones

Webcams and mobile phones can be used to take images without people's knowledge. The school's policy is to signpost areas in which webcams are being used so that people know the webcam is there before they enter that area.

Mobile phones that can take and transmit images will not be permitted in areas of the school, such as changing rooms or sports facilities, where they could be misused. Misuse will be regarded as a breach of school discipline and dealt with accordingly.

External photographers and events

If the school invites or permits an external photographer to take photographs within school, we will:

- Provide a clear brief for the photographer about what is considered appropriate in terms of content and behaviour
- Issue the photographer with identification which must be worn at all times
- Let children and parents know that a photographer will be in attendance at an event and ensure they consent to both the taking and publication of films or photographs
- Not allow unsupervised access to children or one-to-one photo sessions at events.

The same conditions will apply to filming or video-recording of events.

Photographs taken by journalists are exempt from the Data Protection Act as newspapers are subject to strict guidelines governing the press. However, wherever possible and practicable, we will secure parental permission before allowing journalists to take photographs of pupils.

Use of digital images

To comply with the Data Protection Act 1998 we need parental permission to use photographs or recordings of any child.

When posting images for external use, we will avoid using surnames.

If showcasing digital video work to an external audience, we take care to ensure that pupils are not referred to by name on the video, and that full names are not given in the credits at the end of the film.

Only images of pupils in suitable dress will be used.

Staff are not allowed to take photographs or videos on their own personal equipment.

In school we often use digital images during a learning activity. These may be displayed on our website which is public facing so could potentially viewed by anyone on the internet. They may also be displayed on our virtual learning environment which is private to the school community and can only be viewed by those with a username and password.

We would like to ask your permission to use digital images in school.

We would also request that parents respect the privacy of other families and do not post images including other children taken at school events both in and out of school, without permission from other parents/carers.

Use of digital images- photography and video

I agree to the school using photographs/videos of my child

_____ (name)

On the public facing website: **yes/no** (please circle)

On the privately accessed VLE: **yes/no** (please circle)

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.

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

This page has been left blank intentionally

The Legal Framework

Communications Act 2003(section 127)
Sending by means of the internet a message or other matter that is offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction to imprisonment.

NB an offence is committed as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990
Regardless of an individual's motivation, the act makes it a criminal offence to:

- Gain access to computer files or software without permission
- Gain unauthorised access as above in order to commit a further criminal act
- Impair the operation of a computer or program (for example caused by viruses or denial of service attacks)

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission.

Data Protection Act 1998
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data.

Education Act 2011 (sections 2-4)
This clarifies statutory powers to discipline pupils for inappropriate behaviour or for not following instructions both on and off the school premises. Details for free schools can be found in section 36 and Academies in part 6 sections 55-65.

Education and Inspections Act 2006 (sections 90-91)
This provides powers to discipline pupils for inappropriate behaviour or for not following instructions both on and off the school premises. It also gives schools the powers to confiscate items from pupils.

These powers are particularly relevant to online bullying and e-safety as well as giving legal powers to confiscate mobile phones and other mobile devices, if they suspect that they are being used to compromise the well-being and safety of others.

Malicious Communications Act 1988 (section1)
This makes it a criminal offence to send electronic messages that conveys indecent, grossly offensive, threatening material or information that is false. This includes if the message is of an indecent or grossly offensive nature and if the purpose was to cause a recipient to suffer distress or anxiety.

Obscene Publications Act 1959 and 1964 (section 1)
Publishing an 'obscene' article is a criminal offence. This includes electronic transmission.

Public Order Act 1986 (sections 17-29)
This makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. It also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the UK. A child is anyone under 18. Viewing an indecent image of a child on your computer means that you have made a digital image.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which they know or ought to know amounts to the harassment of others.

A person whose course of conduct causes another to fear on at least 2 occasions, that violence will be used against them is guilty of an offence if they know or ought to know that their course of conduct will cause the other to fear on each of these occasions.

The Equality Act 2010
This consolidates discrimination law covering all types of discrimination that are unlawful. It defines that schools cannot unlawfully discriminate against pupils because of their sex, race, disability, religion or belief and sexual orientation. Protection is now extended to pupils who are pregnant or undergoing gender reassignment.

Regulation of Investigatory Powers Act 2000
This regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication.

The Telecommunications (Lawful Business Practice) (Interception of Communications Regulations 2000) does permit a degree of monitoring and record keeping for example in schools to investigate unauthorised use of the network. However all monitoring is subject to consent.

Sexual Offences Act 2003
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice and intentionally meet them or travel with the intent to meet them to commit a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Any sexual intercourse with a child under 13 is considered rape.