Communication and On-Line Safety Policy including Use of Mobile Devices for pupils, Staff, Governors and Visitors

Policy Review Date: 4 July 2024
Date of Next Review: July 2025

At St Gibert of Sempringham Church of England Primary School we recognise the educational benefits of internet access. We believe that the Internet is a powerful tool which should used with good planning and management to ensure appropriate and effective pupil use. We are aware of the potential risks and aim to manage these risks with a balanced approach through robust technical solutions and regulation. Whilst regulation and technological solutions are very important their use must be balanced by teaching pupils to take a responsible approach, and this forms an essential part of the School's On-line safety provision.

It is the duty of the school to ensure that every child in our care is safe and we extend the same philosophy to the virtual or digital world. This document is drawn up to protect all pupils and staff. The school aims to provide clear advice about how to minimise risks and how to deal with any infringements. This policy will be reviewed regularly to reflect the current and emerging technology available. As part of the school's On-line safety education, children will be taught about the potential risks and how to keep personal information safe. This will be through dedicated lessons in ICT/PSHE and follow up assemblies, and On-line safety events. Information will be placed on the school website for parents and carers.
Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children:

- The Internet
- Email
- Blogs
- Instant messaging (eg. Messenger/Skype often with a web cam)
- Podcasting (radio or audio broadcasts)
- Social networking sites (facebook/ twitter/ snapchat)
- Video broadcasting sites (Youtube/Iplayer/ 4OD)
- Internet enabled gaming consoles (playstation, Xbox, Wii)
- Chatrooms
- Gaming Sites
- Music download sites
- Mobile/ Smart phones with camera/video/email/internet functionality

How will the internet provide effective learning?

The purpose of internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management of information and business administration systems. Internet access provides many high-quality teaching and learning resources, some free, some subscription, as well as providing huge potential for research.

How will internet access be authorised?

Internet access will be granted to a whole class or individuals as part of a scheme of work, after suitable education in responsible internet use. Older pupils may carry out their own internet searches for research purposes and should know how to conduct searches safely and what to do if they come across something unsuitable.

Pupils' entitlement to use the internet is based on their responsible use of it. Irresponsible use may result in this privilege being removed.

How will the school ensure internet access is as safe as is reasonably possible?

Our approach to On-line safety is thorough and robust. Staff will:

- ensure that all staff read this policy carefully and all details are understood.
- complete regular On-line safety training.
- accept terms of the acceptable use policy for staff *(Appendix C)*
- post rules of Internet access in their classroom and refer to them regularly

Levels of access and supervision will vary according to pupil's age and experience.

The responsibility for On-line safety is that of the Senior Leadership Team who will:

- Ensure compliance with the policy
- Arrange annual training
- Review filtering systems
- Check internet usage by staff and pupils
- Keep up to date with issues and guidance with organisations such as BECTA and CEOP and appreciate that it is an ever-changing environment.
- Ensure that governors are updated and knowledgeable.
- Ensures On-line safety incidents are dealt with promptly and appropriately.
- Maintaining a log of On-line safety incidents
- Liaise with school technical staff as required

The School employs the services of an external I.T. Provider: Ark ICT. Ark ICT provide the School with an ICT Technician who will:

- ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- ensure that the school meets the required On-line safety technical requirements
- ensure that users may only access the networks and devices through a properly enforced password protection policy
- maintain the filtering policy and update it on a regular basis
- Ensure that monitoring software/systems are implemented and updated as agreed

Our pupils have a responsibility to ensure that they use the internet as safely as possible. Pupils will:

- accept terms of the On-line safety rules for their Key Stage *(Appendix A)*
- demonstrate full compliance with the above
- understand that internet access will be regularly monitored
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will help parents to understand these issues through parents' evenings, newsletters, letters, website and local On-line safety campaigns. Parents and carers will be encouraged to support the school in promoting good On-line safety practice. Parents will:

- Accept terms of the On-line safety rules for their child/ children *(Appendix A)*
- Inform school if they have and concerns regarding On-line safety.

Further guidance for children regarding electronic communication can be found on our website and Appendix B.

How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. Methods to identify, access and minimise risks will be reviewed regularly by the Ark ICT Technician and the Senior Leadership Team.

Our policy deals with 3 areas of risk: Content, Contact and Conduct.

Content

Internet

Pupils are taught what internet use is acceptable and given clear objectives for its use. Internet access will be planned to enrich and extend learning activities. Access levels reflect the curriculum requirements and age of pupils. Currently we operate a filtering system through Ark ICT appropriate to the age of our children. Staff will guide pupils in online activities that will support the learning outcomes

planned for the pupil's age and maturity. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. They will be taught to acknowledge the source of information used and respect copyright when using material accessed on the internet. To ensure that the use of Internet derived material used by staff and pupils complies with copyright law. Pupils are taught to be critically aware of the materials they read and are shown how to validate information before accepting it accuracy. In all areas of the curriculum staff will reinforce On-line safety messages. Pupils are taught about websites that could have a negative/damaging impact on them as part of their On-line safety curriculum lessons and discussions. They are taught to assess the information available for bias and factual accuracy. Pupils are also encouraged, whilst thinking about the benefits of online activity, to think about the amount of time they spend on-line in relation to their health and wellbeing.
If staff or pupils discover unsuitable sites, the URL and content must be reported to the internet service provider by the On-line safety Coordinator.

Use of Film
Recommended age guidance is always followed. Parents are consulted if pupils are watching films that have a PG rating and given the opportunity to watch the films before they are shown to their children. Parents have the right to withdraw their child from these films if they wish.

Contact

Email
Pupils will only use approved email accounts on the school system. Pupils must immediately tell a teacher if they receive offensive email (report to teacher button). Pupils should not reveal details of themselves or others in email communication. E-mails should be carefully written and are monitored by staff.
Pupils are taught at an age-appropriate level, that there are people who could potentially cause them harm. They are taught never to give out personal information when commenting on blogs etc and how to report any information they are worried about. Children are not allowed access to Chat rooms.

Conduct

Pupils and staff should adhere to the acceptable use agreements. All pupils have individual passwords for the school computers. Their teacher keeps a copy of their passwords and the children are taught not to share them, in order for any 'on-line activity' to be accountable to that pupil.

Inappropriate conduct will result in a discussion with a member of the Senior leadership Team/DSL.

If pupils break the agreement their parents will be informed as soon as possible, and records will be kept.

Pupils will be encouraged to consider the nature and possible effects of any misuse of technologies. Their digital footprint and online reputation will be discussed.

Internet or computer privileges may be removed for a specific period of time.

How will publishing on the web be managed?

The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

The point of contact on the school website should be the school address, school email and telephone number. Staff or pupils' home information will NOT be published.

Photographs used on the website must not identity individual pupils by name. Group shots or pictures taken over shoulders will be used where possible and other carefully selected shots (not passport style images).

Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

On entry to our school, written permission from parents/carers will be obtained before photographs are published on the school website. Parent/Carers do NOT have to give permission for their child's photograph to be used on the school website; school will NOT use a child's photograph without parental consent. In line with GDPR, parents may, at any time withdraw their consent for their child's photograph or electronic image to be published on the school website.

Where audio and video are included, the nature of the items uploaded will not include content that allows the pupils to be identified.

Protecting personal data.

Personal data will be recorded, processed, transferred and made available in accordance with GDPR and DPA and other related legislation. The School will:

- ensure that appropriate security measures are in place and enforced to keep paper and electronic personal data secure
- regularly review the physical security of the School buildings and storage systems
- ensure that only authorised individuals have access to personal data
- that all portable electronic devices containing personal data will be encrypted.
- ensure that no personal data will be left unattended in any vehicles and staff will ensure that if it is necessary to take personal data from School premises, for example to complete work from home, the data is suitably secured
- refer to any relevant guidance and seek advice where necessary if processing personal data utilising a cloud-based solution

How will e-mail be managed?

Pupils may only use approved e-mail accounts on the school system. Whole class or group email addresses should be used at KS1 and monitored accounts at KS2, where incoming and outgoing messages are checked and authorised by the teacher before sending or receiving thus all pupils' emails will be treated as 'public'.

Pupils should use email in an acceptable way (being polite and considerate), and must immediately tell a teacher if they receive offensive or distressing messages.

Pupils must make sure they do not reveal any personal details about themselves or others in any online communication, or arrange to meet anyone they meet online.

Information will be provided to parents explaining how pupils can access their accounts from home.

Social networking

Social networking sites and personal emailing such as Twitter, MSN, Facebook, Hotmail, TikTok, Snapchat, Skype, blogs etc are NOT allowed to be accessed by pupils in school.

As part of the School's On-line safety education programme pupils and parents will be advised that social networking sites are inappropriate for primary aged children, pupils in KS2 will be taught about the potential risks and how to keep personal information safe. The purpose of this is to acknowledge (although not to condone) the reality that some children may already have access to social networking sites by this age.

Staff may use such sites that are allowed by Ark ICT filtering system but only when not teaching lessons. Any digital communication between staff and pupils or parents (e-mail/chat) should be professional in content.

Each year group will have specific ICT/PHSEE lessons dedicated to On-line safety, as well as follow up assemblies.

Parents/Carers

Parents/Carers must not put comments, blogs or tweets on social media regarding incidents or concerns relating to pupils, staff or other parents. All matters relating to school should be brought to the attention of the Office Administration Team, Class Teacher or Headteacher.

Mobile Phones/Devices

Introduction and aims

At The St Gilbert of Sempringham C of E Primary School we recognise that mobile devices, including smart phones, are an important part of everyday life for our pupils, parent and staff, as well as the wider school community.

Our policy aims to:

- promote, and set an example for, safe and responsible phone use
- set clear guidelines for the use of mobile devices for pupils, staff, parents and volunteers
- support the school's other policies, especially those related to Safeguarding and Child Protection, Behaviour and Anti-Bullying

This policy also aims to address some of the challenges posed by mobile devices in school, such as:

- risks to Child Protection
- data protection issues
- potential for lesson disruption
- risk of theft, loss, or damage
- appropriate use of technology in the classroom

Pupils

Pupils are not permitted to use or carry mobile devices within school, this includes watches that have the facility to record, photograph and/or receive and send messages. If a parent wishes a child to carry a mobile device to and from school, the device should be handed into the school office for safe keeping upon arrival to school. However, appropriate use of mobile devices will be taught to pupils as part of PSHEE.

Staff

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, send texts, or use their mobile phone or device, (including watches), for any other purpose while children are present/during contact time. Use of personal mobile devices must be restricted to non-contact time, and to areas of the school where children are not present (such as the staff room). Watches which connect to mobile phones should not be worn when working with children

There may be specific circumstances in which it is appropriate for a member of staff to have access to their device during contact time, e.g.

- for emergency contact by their child
- in the case of acutely ill dependants or close family members

in such circumstances, a request must be made directly to the Headteacher. The Headteacher will decide on a case-by-case basis whether to allow for special arrangements.

If special arrangements are not deemed necessary, school staff can use the school office 01529 240465 as a point of emergency contact.

Data protection

Staff must not use their personal mobile devices to process personal data, or any other confidential school information.

Safeguarding
Staff must refrain from giving their personal contact detail to parents or pupils, including connecting through social media and messaging apps.

Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents or pupils.

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) must not use their mobile device to take photographs or recordings of pupils, their work or anything else which could identify a pupil. If it is necessary to take photographs or make recordings as part of a lesson/school trip/activity, this must be done using school equipment.

Using personal devices for work purposes
In some circumstances, it may be appropriate for staff to use personal mobile devices for work. Such circumstances may include but are not limited to:

- emergency evacuations
- supervising off-site trips
- supervising residential visits

In these circumstances, staff will:
- Use their mobile device in an appropriate and professional manner, in line with our staff code of conduct
- Not use their device to take photographs or make recordings of pupils, their work, or anything else that could identify a pupil
- Refrain from using their mobile device to contact parents unless there is an urgent situation whilst on a school trip or residential trip. Where practical, contact will be made through the school office

Sanctions
Staff who fail to adhere to this policy may face disciplinary action. See the school's staff disciplinary policy for more information.

Use of mobile devices by parents, volunteers and visitors

Parents, visitors and volunteers (including governors and contactors) must adhere to this policy as it relates to staff if they are on the school site during the school day.
This means:

- not taking pictures of recordings of pupils, unless it is a public event such as Sports' Day, Sponsored Walk, or of their own child
- using any photographs or recordings for personal use only, and **not** posting on social media
- not using mobile devices in lessons, or when working with pupils

Parents, visitors and volunteers will be informed of the rules for mobile device use when they sign in at reception or attend a public event in school. (*See Appendix D Photographs and Digital Recordings and Appendix E Mobile phone information slip for visitors).*

Parents or volunteers assisting in supervising a school trip must not:

- use their device to make contact with other parents
- take photographs or recordings of pupils, their work, or anything else which could identify a pupil

Parents must use the school office as the first point of contact if they need to get in touch with their child during the school day. Parents must not try and contact their child on his/her personal device during the school day.

How will staff and parents be informed about On-line safety?

All staff will have access to this On-line safety Policy, and its importance explained with relevant training given and they will sign the ICT Acceptable Use Policy.

The On-line safety Co-ordinators will provide advice/guidance/training as required and keep up to date on relevant issues.

All staff will take part in On-line safety training provided by the Deputy Safeguarding Leads or other relevant organisations.

The school will seek to draw attention to the school's School On-line safety Policy and provide information and awareness of key On-line safety issues to parents/carers through newsletters and the school website.

How will complaints be handled?

Owing to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or device. Neither the school nor the Local Authority can accept liability for material accessed or any consequences of internet access.
Responsibility for handling any incidents will be given to the Headteacher or delegated as the need arises.

Complaints about misuse of the internet in school by pupils must follow the most relevant school policies (i.e. Behaviour, Anti-Bullying, Anti-Racism, Health and Safety).

Monitoring and reviewing

This policy will be monitored annually and will be reviewed as the need arises or at the review date given.

Review date September 2024

Appendix A

St Gilbert of Sempringham Church of England Primary School

Rules for Acceptable Use for Foundation and KS1

- I always ask a teacher or adult if I want to use the computers, laptop or tablets.
- I only open activities that an adult has told or allowed me to use.
- I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- I keep my passwords safe and will never use someone else's
- I know personal information such as my address and birthday should never be shared online.
- I know I must never communicate with strangers online.
- I am always polite and friendly when I post to our blogs, use our email and other communication tools, with our teachers help.

Appendix A continued

St Gilbert of Sempringham Church of England Primary School

Rules for Acceptable Use for KS2

- I will ask permission before using computing equipment.
- I will use the school ICT and Internet for school work and homework that the teacher has asked me to do.
- I will not deliberately look for, save or send anything which might make others upset.
- I will tell an adult if I see anything I am uncomfortable with, or I know is inappropriate.
- I will never give out personal information or passwords.
- I will only use my own usernames and passwords and log off when I have finished using the computer.
- I know that the school checks my files and the online sites I visit. I will not try to bypass any of the security measures in place.
- I will respect the computing equipment and tell an adult if I notice something isn't working correctly or damaged.
- I will use all communication tools carefully and tell an adult if someone who isn't approved by a teacher is messaging.
- I know that I am not allowed on any personal e-mail, social networking or instant messaging in school.
- At school, I may not download any software from the internet or bring a personal memory stick into school.

- Before I share, post or reply to anything online, I will THINK. Is it true? Is it helpful? Is it inspiring? Is it necessary? Is it kind?

- I understand that if I behave negatively whilst using technology, my parents/carers will be informed and there will be consequences for my actions.

Appendix B

Advice for children regarding electronic communications.

- Treat your password like your toothbrush – Keep it to yourself!

- Only give your mobile number or personal e-mail address to trusted friends.

- Block the bully – learn to block or report someone who is behaving badly.

- Save the evidence – learn how to keep records of offending text messages, pictures or online conversations.

- Don't retaliate or reply.

- Check your profile and make sure it doesn't include any personal information.

- Always respect others – be careful what you say online and what images you send.

- Think before you send – whatever you send can be made public very quickly and could stay online for ever.

- Look out for your friends – and do something if you think they are at risk.

- Tell your parent, carer or a teacher if something or someone makes you feel uncomfortable or worried.

Appendix C

Rules for Acceptable Use Policy (School staff)

Internet Access

You must not access or attempt to access any sites that contain any of the following: child abuse, pornography, promoting discrimination of any kind, promoting racial or religious hatred, promoting illegal acts, any other information which may be illegal or offensive to colleagues. It is recognised that under certain circumstances inadvertent access may happen. Should you access any of these sites unintentionally, you should report the matter to Mrs Foston, so that it can be recorded in the logbook.

Social Networking

Staff use of social networking sites is not permitted in school time. If you choose to use social networking sites out of school hours, you should fully acquaint yourself with the privacy settings that are available on any social networking profile in order that profiles are not publicly available. Staff using social networking for personal use should never undermine the school, its staff, parents or pupils. All staff should be careful about who they become friends with and how they conduct themselves on social networking sites. School staff must not accept current pupils at this school as friends on social networking sites.

Use of E-mail

All members of staff should use their professional email address for conducting school business only. Use of school email for personal/social use is at the discretion of the Headteacher. Emails should be written carefully, politely and professionally. Users are responsible for the email they send and for contacts made.

Passwords

Staff should keep passwords private. Passwords are confidential and individualised to each person. On no account should you allow a pupil to use your login.

GDPR and Data Protection

Where you have to take home sensitive or confidential information, sufficient safeguards should be in place to prevent loss or misuse. If it is necessary to take work home, or off site, you should ensure that the device) laptop, USB pen drive, iPad) is encrypted. On no occasion should data concerning personal information be taken off site on an unencrypted device.

File Sharing

Technology such as peer to peer and bit torrents is not permitted on the Lincolnshire School's Network.

Personal Use

Personal use of ICT equipment is permitted, but should not be abused for example, during lesson times. Use for personal financial gain, gambling, political purposes or advertising is not permitted. It must also be stringently checked for up to date anti-virus and malware checkers. ICT system security must be respected. Using a computer for a purpose not permitted by the system owner could constitute a criminal offence under the Computer Misuse Act 1990.

Images and Videos

You are not allowed to take photographs of pupils or pupils' work on your own personal phones/cameras etc. You must also not upload onto any internet site images or videos of yourself, other staff or pupils without consent. Neither should they be uploaded onto your personal computer.

Mobile Devices

Mobile devices must not be used during times of contact with children. During school hours, mobile devices may only be used within areas where children are not present. These devices should have adequate password protection on them should they be accessed by an unauthorised person.

Viruses and other malware

Any virus outbreaks should be reported to the office staff as soon as it is practicable.

School computer systems may be subject to monitoring, including access to websites and the interception of email.

I have read and agree to abide by the above policy.

Signed: _____ Date: _____

Appendix D

Photographs/Digital Recordings at school performances/school assemblies

During the School Performance/School Assembly, it is likely that many of you intend to make recordings or take photographs of your child as a special memento. However, with the growing popularity of internet sharing websites, we should make you aware of the safety implications to your child and other children, should you choose to publish photographs of your child online.

Modern technology means it is very easy to distribute images world-wide via websites such as Facebook. Sometimes, without intending any offence, it is possible to 'publish' photos that include other people's children. The parents of those children may not be happy about images being published on the web. There may even be legal reasons for these photos to not be made public.

Whilst it would be unreasonable to ban all photography and recordings at such events, we do ask that if you intend to take photographs or make recordings that you are aware of the responsibilities, not only towards your children, but to the children of others.

We ask that if any photographs/recordings are published through a social networking website or other internet sharing site that you are considerate and understanding if images of other people's children are involved. For the safety of the children, they should not be 'tagged' in photographs from school events; neither should their full names, names of any other children or the name of our school be published. It should be noted that whilst it is permissible under the Data Protection Act 1998 to take photographs for personal use, publication of such images may be unlawful.

We hope you understand the need for sensible use of photographs and recordings involving children from our school, and whilst we discourage publishing photographs of children online we ask that you are considerate to others if you do decide to publish your photographs/recordings.

Please Note: Finally, if you intend to make a video recording of the School Performance, please let a member of staff know in the school office so that a log of the recording can be made.

Appendix E

Mobile device information slip for visitors

Use of mobile devices in our school

- **Please keep your mobile devices on silent/vibrate while on school grounds**
- **You must not use mobile devices where pupils are present, (including iwatches). If you must use your phone, you may go to the Staff Room**
- **Do not take photographs or make digital recordings of pupils, pupils work or staff**
- **Do not use your mobile device in lessons, or when working with pupils**

The school accepts no responsibility for devices that are lost, damaged or stolen whilst you are on the school grounds

A full copy of the *Communication, On-line safety and Internet Policy including Use of Mobile Devices for Pupils, Staff, Governors and Visitors – September 2023* is available from the school office.

Mobile device information slip for visitors

Use of mobile devices in our school

- **Please keep your mobile devices on silent/vibrate while on school grounds**
- **You must not use mobile devices where pupils are present, (including iwatches). If you must use your device, you may go to the Staff Room**
- **Do not take photographs or make digital recordings of pupils, pupils work or staff**
- **Do not use your mobile device in lessons, or when working with pupils**

The school accepts no responsibility for phones that are lost, damaged or stolen whilst you are on the school grounds

Communication, On-line safety and Internet Policy including Use of Mobile Devices for Pupils, Staff, Governors and Visitors – September 2023 **is available from the school office.**