St Herbert's RC Primary School

E-SAFETY POLICY

Approved by Governors on: 4th December 2023

Date to be reviewed: Spring 2025

Signed on behalf of the Governing Body: *P Devine (Chair)*

Contents

OVERVIEW

This policy is set within the context of the School Mission Statement:

"Strong in Faith, Hope and Love, for the Common Good"

and the School Ethos:

"By loving one another as God loves us, we can achieve spiritually and academically"

1. Introduction

ICT and computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook, Twitter and Instagram
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually age 12+ / at least 13 years of age.

At St Herbert's RC Primary School, we understand our responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of technologies provided by the school (such as PCs, iPads, tablets, laptops, mobile devices, webcams, interactive displays, digital video equipment, etc) and technologies owned by contractors, visitors and governors, but brought onto school premises (such as laptops, iPads, tablets, mobile phones, and other mobile devices).

2. Monitoring

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Regulations 2018, or to prevent or detect crime.

All monitoring, surveillance or investigative activities are conducted by the Headteacher and ICT authorised staff in compliance with the General Data Protection Regulations 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

In order to safeguard all pupils and staff, all school owned devices are enrolled into a web content filtering and monitoring system that continually filters and monitors the internet traffic, wherever the device is connected to the internet.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

3. Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Any internal or external data breaches must be reported in line with the GDPR (Data Protection) Policy.

4. Acceptable Use Agreement: Pupils - Primary

Educational use of the Internet is characterised by activities that provide children with appropriate learning experiences. Clear rules which help children develop a responsible attitude to the use of the Internet have been devised. Clear expectations and rules regarding use of the Internet will be explained to all classes. A copy of them is sent home to the parents of any new child and a simplified version is also displayed within school to ensure that everybody is made aware of them.

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and my parents/ carer contacted if a member of school staff is concerned about my e-Safety.
- I understand that my own device (smart phones, watches etc) cannot be used in school.

5. Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life. This policy is designed to ensure that 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. Any concerns or clarification should be discussed with the e-Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher 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 will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the ICT Technician Manager, other than software updates of devices issued to me, in order to ensure their functionality and security.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I understand that all my 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 Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

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

Signature: _____ Date: _____

Full Name: _____ (printed)

Job title: _____

6. Computer Viruses

Never interfere with any anti-virus software installed on school ICT equipment that you use.

If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your ICT Technician Manager.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT Technician Manager immediately, who will advise you what actions to take and be responsible for advising others that need to know.

7. E-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. As part of the Computing curriculum, pupils must have experienced sending and receiving e-mails.

7.1. Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher and Line Manager.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- You must therefore actively manage your e-mail account as follows:
    - Delete all e-mails of short-term value.
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives.
- The forwarding of chain letters is not permitted in school.
- All pupil e-mail users are expected to adhere to the generally accepted rules of 'netiquette', particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive email.
- Staff must inform the e-Safety co-ordinator if they receive an offensive e-mail.

- Pupils are introduced to e-mail as part of the Computing Scheme of Work
- However you access your school e-mail (directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

7.2. Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section e-mailing Personal, Sensitive, Confidential or Classified Information.
- Use your own school e-mail account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- School e-mail is not to be used for personal advertising.

7.3. Receiving e-Mails

- Check your e-mail regularly.
- Activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source; Consult your network manager first.
- All attachments must be virus checked before opening.
- Do not use e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding and deletion of e-mails is not allowed.

7.4. E-mailing Personal, Sensitive, Confidential or Classified Information

- Where your conclusion is that e-mail must be used to transmit such data:
    - Obtain express consent from your manager to provide the information by email.
    - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
        - Encrypt and password protect attachments.
        - Verify the details, including accurate e-mail address, of any intended recipient of the information.
        - Verify (by phoning) the details of a requester before responding to e-mail requests for information.
        - Do not copy or forward the e-mail to any more recipients than is absolutely necessary.
    - Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone).
    - Send the information as an encrypted document **attached** to an e-mail.
    - Provide the encryption key or password by a **separate** contact with the recipient(s).
    - Do not identify such information in the subject line of any e-mail.
    - Request confirmation of safe receipt.

8. Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's e-Safety rules.

However, staff are aware that some pupils may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

9. E-Safety

9.1. E-Safety - Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in this school is Mrs S. Milligan who has been designated this role as the Headteacher. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as OCC LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Headteacher / e-Safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: safeguarding & child protection, health and safety, home–school agreements, behaviour / pupil discipline (including the anti-bullying) policy and PSHE.

9.2. E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

- The school has a framework for teaching internet skills in ICT/ PSHE lessons.
- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the relevant legislation when using the internet, such as data protection and intellectual property, which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

- Pupils are taught about keeping safe online in line with the 'Keeping Children Safe in Education' September 2022 document and the Prevent duty.

9.3 E-Safety Skills Development for Staff

- Our staff receive regular information and training on e-Safety and how they can promote the 'Stay Safe' online messages.
- Details of the ongoing staff training programme can be found in the school inset programme.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

9.4. Managing the School E-Safety Messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-Safety policy will be introduced to the pupils at the start of each school year.
- E-Safety posters will be prominently displayed.
- The key e-Safety advice will be promoted widely through school displays, newsletters, class activities etc.

9.5. E-Safety Training for Parents

The school understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

For these reasons, the school provides opportunities for parents/carers to receive e-safety education and information (e.g. via the school website and information evenings) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good e-Safety behaviour – this includes delivery via newsletters and the school website.

10. Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's e-Safety Co-ordinator.

Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the e-Safety Co-ordinator.

10.1. E-Safety Incident Log

All e-safety incidents must be logged on CPOMs.

10.2. Misuse and Infringements

Complaints

Complaints and / or issues relating to e-Safety should be made to the e-Safety co-ordinator or Headteacher.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Staff must report any e-safety incidents in relation to the Prevent Duty following our safeguarding procedures.

11. Internet Access

The Internet is an open worldwide communication medium, available to everyone at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

11.1. Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile Internet connectivity.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- Staff must report any e-safety incidents in relation to the Prevent Duty following our safeguarding procedures.

11.2. Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application.
- On-line gambling or gaming is not allowed.
- It is at the Headteacher's discretion as to what Internet activities are permissible for staff and pupils and how this is disseminated.

11.3. Infrastructure

- Web-based activity is monitored and recorded using Lightspeed Systems Filter, a web based system in line with the Keeping Children Safe in Education document of September 2023.
- School Internet access is controlled through our web filtering service provided by Lightspeed Systems in line with the Keeping Children Safe in Education document of September 2023. Any activity online by pupils that falls under the categories of self harm, bullying etc will raise an alert from the Lightspeed Alert system to the designated staff who can act on this quickly to ensure the safety of pupils. There is also a human review team at Lightspeed who monitor the activity and will contact the designated staff directly if they see a potential for serious harm to a pupil.

- St Herbert's RC Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; General Data Protection Regulations 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to Internet logs.
- The school uses management control tools for controlling and monitoring workstations, laptops & tablets.
- If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to the ICT Technician Manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility, nor the ICT Technician Manager to install or maintain virus protection on personal systems.
- Pupils are not permitted to download programs or files on school based technologies.
- Staff are permitted to download appropriate free Apps on their school issued devices for testing and evaluation purposes, then an email request must be made to the ICT Technician Manager to deploy the App to the pupil and/or staff devices.
- If there are any issues related to viruses or anti-virus software, the ICT Technician Manager should be informed.

12. Managing Other Web 2 and upcoming Web 3 Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking and online games websites to pupils within school.
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on websites, which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our pupils are asked to report any incidents of Cyberbullying to the school.
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform, website or other systems approved by the Headteacher.

13. Parental Involvement

The School believes that it is essential for parents / carers to be fully involved with promoting e-Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies together with the associated risks.

- Parents / carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-Safety policy.
- Parents / carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.
- Parents / carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g. on school website).
- Parents / carers are expected to sign a Home School agreement containing the following statement or similar:

  "We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or video that could upset or offend any member of the school community."
- The school disseminates information to parents relating to e-Safety where appropriate in the form of:
  - Information and celebration evenings.
  - Practical training sessions e.g. How to adjust the Facebook privacy settings.
  - Posters.
  - School website.
  - Newsletter items.
  - X
  - Email
  - SMS text messaging

14. Passwords and Password Security

14.1. Passwords

- **Always use your own** personal passwords.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else.** Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- **Never tell a child or colleague your password.**
- **If you are aware of a breach of security with your password or account inform the ICT Technician Manager immediately.**
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols.
- User ID and passwords for staff and pupils who have left the school are suspended immediately and removed after a designated period.
- As staff members leave, passwords for shared online resources must be changed immediately.

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT Technician Manager.

14.2. Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords that are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security.
- Users are provided with an individual network, email, learning platform and Management Information System (where appropriate) log-in username, from which they are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically.

- Individual staff users must also make sure that workstations / laptops are not left unattended and are locked.
- Due consideration should be given when logging into online applications to the browser / cache options (shared or private computer).

14.3. Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorised access.
- Regularly change generic passwords to avoid unauthorised access (Microsoft© advise every 42 days).

15. Safe Use of Images

15.1. Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. (Note that school allocated mobile devices will be made available to record and transmit photographs and videos of school trips).
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher.
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication.

15.2. Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school website.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- Recorded/ transmitted on a video or webcam.
- On any of the school's other online resources (eg: School Facebook and Twitter)
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, ie exhibition promoting the school.
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically) unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Uploading to the sites can only happen with express permission from the Headteacher.

15.3. Storage of Images

- Images/ films of children are stored on the school's network and cloud services such as Google Drive, Tapestry & Evernote.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks).
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource.
- The Computing Lead & Technician Manager has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

15.4. Webcams

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images

15.5. Video Conferencing (Facetime, Google Hangouts & Skype)

- Permission is sought from parents and carers if their children are involved in video conferences.
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing.
- All pupils are supervised by a member of staff when video conferencing with endpoints beyond the school.
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

16. ICT Equipment

16.1. School ICT Equipment

- As a user of the school ICT equipment, staff are responsible for their own activity.
- The school logs ICT equipment issued to staff and records serial numbers as part of the school's Asset Management Policy.
- Staff should not allow their visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.
- Staff should ensure that all ICT equipment that they use is kept physically secure.
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- It is imperative that you save your data on a frequent basis to the school Google Drive and / or Tapestry / Evernote.
- Personal or sensitive data should not be stored on the local drives of desktop PC, iPads, laptop, or other portable device.
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.
- Privately owned ICT equipment should not be used on a school network unless provision has been made via the Technician Manager.
- On termination of employment, resignation or transfer, return all ICT equipment to your Technician Manager. You must also provide details of all your system logons so that they can be disabled.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All ICT equipment allocated to staff must be authorised by the ICT Technician Manager. Authorising Managers are responsible for:
    - maintaining control of the allocation and transfer within their Unit.
    - recovering and returning equipment when no longer needed.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and GDPR 2018.

16.2. Portable and Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Staff must ensure that all school data is stored on Google Drive, and not kept solely on the laptop / iPad.

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.
- Synchronise all locally stored data, including diary entries, with the cloud services, Tapestry/Evernote and GSuite.
- Ensure portable and mobile ICT equipment is made available as necessary for antivirus updates and software installations, patches or upgrades.
- The installation of any paid applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your Technician Manager. Appropriate free Apps may be downloaded by Staff for evaluation and testing purposes to their school issued laptops and iPads.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

16.3. Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as, Smartphones, iPads & games players are generally very familiar to children outside of school. They often provide a collaborative, well known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

16.3.1. Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use during approved break times in the staffroom or areas of school where pupils are not present. Under no circumstances does the school allow a member of staff to contact a pupil or parent / carer using their personal device.
- Personal devices should not be connected to the school IT system without prior approval.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- No images or sound recordings are permitted on these devices.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

16.3.2. School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.

- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and iPads for off site visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

17. Social Networking and Messaging Systems

The school recognises that many staff will actively use *Facebook*, *Twitter* and other such: social networking, blogging and messaging services, including supporting their own professional development by developing personal learning networks with other educational practitioners.

Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks – discretion and professional conduct is essential. They are encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

Staff must be made aware that it is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors.

Staff should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers. All correspondence should be via school systems.

- Our school uses the school website, X and the school text messaging and email service to communicate with parents and carers. Only those authorised by the Headteacher are allowed to post or send messages on these technologies.
- Staff ***are not*** permitted to access their personal social media accounts using school equipment at any time during school working hours***.***
- Staff ***are*** permitted to access their personal social media accounts using their own devices during approved breaks from contact with children in the staffroom or areas where pupils are not present.
- Pupils are not permitted to access their social media accounts whilst at school.
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and videos they post online can be viewed by others, copied and stay online forever.
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

18. Class X Accounts

The aim of using X is to quickly share and celebrate children's achievements, successes and school updates. It also allows teachers to demonstrate safe and responsible use of social media and encourages the use of 21st Century technology.

- The school X accounts will be run from school devices by the Headteacher and Class Teachers.
- The school X accounts will be public accounts. Senior Leaders and the Computing Leader will monitor the followers and block any who appear to not be school focused.
- The school X accounts will only follow educationally linked accounts. No personal accounts, unless they are educationally linked, will be followed. For example a children's author.
- The school X accounts will not reply to any 'replies' on X. This is not the platform to discuss or debate school related issues.
- The school X accounts will only use children's first names when referencing children's work (not images).
- The school X accounts will use X to share positive messages about the school.
- The accounts may be used to share news and information during a school trip. The account will be run by a senior teacher on a 3G/4G connected phone for the period of the trip. Photos taken on the phone for the purpose of sharing on X will be deleted once they have been shared.
- The school will change the X account passwords on an annual basis or as / when staff members leave school.
- Individually targeted content will not be posted e.g. "Well done Josh a better lesson today". X Posts to a year group or class along the lines of "don't forget the..." are acceptable. Also, always think about the most effective way to communicate important information.
- Use of the @Xname of others is to be avoided. For example *" excited about @dexnott speaking to us"* .
- By endorsing X we may be encouraging children to use X so reinforce e-safety rules such as "Never post anything that would be potentially upsetting; make sure you know how to report to anything you find that disturbs you; be careful who you talk to they may not be all they appear; never meet anyone from X world without telling your parents" etc. Remind children they must be 13 years of age to use Twitter.
- X's own safety rules can be read on: https://help.twitter.com/en/resources/a-safer-twitter

19. Mobile Telephone Services

- Staff are responsible for the security of the school mobile phone. They should always set the PIN code on the school mobile phone and not leave it unattended and on display (especially in vehicles).
- Report the loss or theft of any school mobile phone equipment immediately.
- The school remains responsible for all call costs until the phone is reported lost or stolen.
- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it.
- School SIM cards must only be used in school provided mobile phones.
- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default.
- You must not send text messages to premium rate services.
- In accordance with the **Finance policy** on the private use of school provided mobiles, you must reimburse the school for the cost of any personal use of your school mobile phone. This includes call charges incurred for incoming calls whilst abroad. [To assist you in identifying personal use, add * to the end of the number being contacted, these will be shown separately on your bill]. Payment arrangements should be made through your finance administrator.
- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so.

20. Policy Writing and Review

20.1. Staff and Pupil Involvement in Policy Creation

- Staff, governors and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through pupil voice, school council meetings & staff meetings.

20.2. Review Procedure

- There will be on-going opportunities for staff to discuss with the e-Safety coordinator any e-Safety & Data Security issue that concerns them.
- This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.
- The policy will be amended if new technologies are adopted or the Central Government changes the orders or guidance in any way.

21. Current Legislation

Acts Relating to Monitoring of Staff e-Mail

General Data Protection Regulations 2018
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
https://eugdpr.org/the-regulation/

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.legislation.gov.uk/uksi/2000/2699/contents/made

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
https://www.legislation.gov.uk/ukpga/2000/23/contents

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

Other Acts Relating to e-Safety

Racial and Religious Hatred Act 2006
It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an

offence to meet them or travel to meet them anywhere in the world with the intention of committing 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 also 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. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
https://www.legislation.gov.uk/ukpga/2003/42/contents

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly 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. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 - 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- Access to computer files or software without permission (for example using another person's password to access files)
- Unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or

use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 - 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 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 United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other to fear on each of those occasions.

Prevent Duty - Section 29 of the Counter-Terrorism and Security Act 2015
The Prevent duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities, in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

Acts Relating to the Protection of Personal Data

General Data Protection Regulations 2018
https://eugdpr.org/the-regulation/

The Freedom of Information Act 2000
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Appendix 1

Dear Parent/ Carer

ICT and Computing, including the internet, e-mail and mobile technologies, have become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact your child's class teacher.

Yours Sincerely,

Mrs S Milligan
(Headteacher)

Parent/ carer signature

We have discussed this and ……..... (child name) agrees to follow the e-Safety rules and to support the safe use of ICT at St Herbert's RC Primary School.

Parent/ Carer Signature …….……

Class …… Date …….


Childnet International
www.childnet.com
Be Smart on the internet
S
SAFE
Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.
m
MEETING
Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
a
ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
r
RELIABLE
Information you find on the internet may not be true, or someone online may be lying about who they are.
t
TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
You can report online abuse to the police at www.thinkuknow.co.uk
THINK U KNOW
www.kidsmart.org.uk
KidSMART
Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.