St Mary's Catholic Primary School

E-Safety and Acceptable Use of ICT Policy

(February 2018)

Introductory Statement

The internet provides instant access to a wealth of up-to-the minute information and resources from across the world. Use of email, mobile phones and internet messaging applications all enable improved communication and facilitate the sharing of data and resources.

However, the dangers associated with the internet and technology means that it is paramount that we safeguard both pupils and staff at school. Some of the risks which we must seek to reduce include:

- **Children and staff inadvertently accessing content of an unsavoury, distressing or offensive nature on the internet or receiving inappropriate or distasteful emails.**
- **Children and staff receiving unwanted or inappropriate emails from unknown senders, or being exposed to abuse, harassment or 'cyber-bullying' via email, text or instant messaging, in chat rooms or on social-networking websites.**
- **Chat rooms providing cover for unscrupulous individuals to groom children.**

We believe that, when balanced, the social and educational benefits which are gained by using electronic media mean that the advantages far out-weigh the risks, so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practice and behaviour.

Access to these electronic media help ensure:

- **Children and/or young adults are equipped with skills for the future.**
- **Instant access to a wealth of up-to-date information and resources from across the world.**
- **That children's reading and research skills are improved.**
- **That good social and communication skills are fostered and developed.**

This policy, written in accordance with BECTA guidelines, focuses on each individual technology available within our school and outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to.

Procedures for Use of our Shared Network

This section outlines what users must and must not do when using a PC / laptop connected to a network:

- Children must access the network using their own logons.
- Staff must only access the network using their own passwords. These must not be disclosed or shared.
- Visitors (eg- supply staff) wishing to access the network must first read and agree to abide by this e-safety policy.
- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
- Software must not be installed without prior permission from the person responsible for managing the network.
- Removable media (e.g. pen drives / memory sticks, CDs) must be scanned for viruses before being used on a machine connected to the network.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.'
- Machines must be 'logged off' and shut down correctly after use.

Our school has a wireless network which is encrypted to prevent outsiders from being able to access it. This is securely maintained and the password is kept safe by the system administrator.

Procedures for Use of the Internet and Email

This section outlines the procedures for safe internet and email at our school:

- All pupils and staff must sign an Acceptable Use Agreement before access to the internet and email is permitted in the establishment.
- On an annual basis, parental or carer consent is requested in order for children to be allowed to use the internet or email.
- Users must access the internet and email using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's email account.
- Children must be supervised at all times when using the internet and email.
- Procedures for safe internet use and sanctions applicable if rules are broken will be discussed with all children on an annual basis.
- Accidental access to inappropriate, abusive or racist material is to be reported without delay to the Headteacher, ICT Coordinator or ICT Technician and a note of the offending website address (URL) taken so that it can be blocked.
- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk, malware or unwanted correspondence. This is to be reviewed and updated regularly.
- Any email addresses assigned to individual pupils will not be in a form which makes them easily identifiable to others.
- Users must not disclose any information of a personal nature in an email or on the internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.
- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or hateful language of any kind will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- All emails sent from an establishment/service email account will carry a standard disclaimer disassociating the establishment/service and the Local Authority with the views expressed therein.
- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

- **If users are bullied, or offensive emails are received, this must be reported immediately to a trusted adult or member of staff within school. Emails received should not be deleted, but kept for investigation purposes.**

- **Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.**
- **All email attachments must first be scanned before they can be opened.**
- **Pupils must seek permission before downloading any files from the internet.**
- **All users will be made aware of copyright law and will acknowledge the source of any text, information or images copied from the internet.**

Procedures for Use of Social Media

- **Use of Social Media, such as Facebook, is not permitted, bearing in mind that children under the age of 13 cannot subscribe to these sites anyway.**

- **Children, visitors, volunteers in school and staff must not access public or unregulated chat rooms/forums.**

Procedures for Use of Cameras, Video Equipment and Webcams

- **Permission must be obtained from a child's parent or carer before photographs or video footage can be taken. The school uses a standard form to ensure that children have parental permission.**

- **Photographs or video footage must be downloaded immediately and saved into a designated folder. These will be accessible only to authorised members of staff. School cameras and memory cards should remain in school.**

- **Any photographs or video footage stored must be deleted immediately once no longer needed.**

- **The use of staff's own cameras, video recorders or camera phones in school and during a trip or visit is not permitted.**

- **Parents' permission must be secured in order for children to take photographs of their peers (eg – on residential visits and school trips).**

- **Video conferencing equipment and webcams must be switched off (disconnected) when not in use and the camera turned to face the wall.**

- **Webcams must not be used for personal communication and should only be used with an adult present.**

- **Children and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.**

Procedures to ensure safety of the school's website

- **The school has a designated member of staff who is responsible for approving all content and images to be uploaded onto its website prior to it being published.**
- **The school website is subject to frequent checks to ensure that no material has been inadvertently posted, which might put children or staff at risk or cause offence.**
- **Copyright and intellectual property rights will be respected.**
- **Permission will always be obtained from parents or carers before any images of children can be uploaded onto the school website.**
- **Names must not be used to identify individuals portrayed in images uploaded onto the school website. Similarly, if a child or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.**
- **When photographs to be used on the website are saved, names of individuals portrayed therein should not be used as file names. *This may be something which people would often not think twice about doing. If the photographs are not stored in a 'password-protected' folder, individuals can be easily identified or if photographs are uploaded onto a website or downloaded, the file names may be visible.***
- **If the school website contains a guestbook, public noticeboard, forums or weblogs, the designated member of staff who is responsible for approving all content and images on the school website will check this on a weekly basis.**

Procedures for using mobile phones

- **Children who are in Year 5 and Year 6 and who walk to school and home unaccompanied are allowed to bring mobile phones to school. All children are required to switch mobile phones off and hand them into the school office on entry to school.**
- **The taking of still pictures or video footage with mobile phones is forbidden.**
- **Children should not accept files sent via Bluetooth to their mobile phones by an unknown individual. If they do (eg – on the way to school) and the content received is upsetting or makes them feel uncomfortable, they should pass this on to a trusted adult straightaway.**
- **The use of mobile / camera phone for inappropriate or malicious purposes (eg- for the sending of abusive or unsavoury images / text messages or files via Bluetooth, the making of hoax, crank or abusive phone calls, etc.) is forbidden and will be dealt with in accordance with the school's agreed Behaviour Policy.**

Procedures for using wireless games consoles

- **The use of wireless games consoles is not allowed in school but, at the discretion of the headteacher, may be taken on residential visits.**
- **Any unwanted contact received via a wireless games console, which makes children or young adults feel vulnerable or uncomfortable, must be reported immediately to a teacher or other member of staff.**

Procedures for using portable media players

- **The use of portable media players is not allowed in school but, at the discretion of the headteacher, may be taken on residential visits.**

Sanctions to be imposed if procedures are not followed

The steps to be taken if rules are broken, and the types of sanctions the school intends to impose if procedures are not adhered to, include:

- **Letters may be sent home to parents or carers.**
- **Users may be suspended from using the school's computers, internet or email, etc. for a given period of time or even indefinitely.**
- **Details may be passed on to the police in more serious cases.**
- **Legal action may be taken in extreme circumstances.**

Cases of misuse will be considered on an individual basis by the headteacher and sanctions imposed to match the infringement.

Concluding Statement

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into St Mary's and this policy will not remain static. It may be that staff and children might wish to use an emerging technology for which there are currently no procedures in place. The use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates.

Date of Policy adoption: 4th February 2013
Who adopted the policy: RE and Curriculum Standards sub-committee on behalf of the full Governing Body

Date of policy re-adoption: 7th February 2018

Who re-adopted the policy: Safeguarding, Premises and Health and Safety sub-committee, on behalf of the full Governing Body

ICT Acceptable Use Agreement and Code of Conduct for Staff

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all 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 Mr Jon Murray, Headteacher at Saint Mary's Primary School.

- **I will only use the school's email, internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.**
- **I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.**
- **I 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 email address, to pupils.**
- **I will only use the approved school email system for any school business.**
- **I will ensure that personal data (such as data held on SIMS) 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 Head or Governing Body.**
- **I will not install any hardware of software without permission of the SLT.**
- **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 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 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 will respect copyright and intellectual property rights.**
- **I will abide by the school's Use of Social Media Policy and will use social media in a way that will not bring my professional role into disrepute.**
- **I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.**

User Signature

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

Signature …… Date ……

Full Name ……(printed)

Job title . . . . . .

ICT Acceptable Use Agreement and Code of Conduct
For pupils and their parents to sign

This is how we stay safe when we use computers:

- I will ask a teacher or other member of staff before I use the computers / tablets
- I will only take part in activities that a teacher or other member of staff has asked or allowed me to
- I will take care of the computer and other equipment, logging off and shutting down when my session is over.
- I will ask for help from a teacher or other member of staff if I am not sure what to do or if I think I have made a mistake
- I will tell a teacher or other member of staff if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet and that school will inform my parent(s)/carer(s)
- I will share any concerns that I have about my e-safety with a teacher or other member of staff.

Signed (child): .....

Signed (parent): .....

Date: .....