"Christ's ministry, as recounted in the Gospels, and the values he promoted through his teachings are fundamental to the life of our school in fulfilling its purpose as a Catholic institution." (Mission Statement)

E-Safety and Acceptable Use Policy

June 2022

The staff at St. Aidan's Catholic Primary School strongly believes in the educational value of electronic services and recognises their potential to support the curriculum. Every effort will be made to provide quality experiences to children and teachers using this information service, however, inappropriate and/or illegal interactions with any information service are strictly prohibited.

Listed below are the provisions of this agreement. If any student violates these provisions, access to the internet will be denied and the children will be subject to disciplinary action.

1. Internet Safety:

    - The school will appoint an E-Safety Coordinator. This may be the Child Protection Liaison Officer as the roles overlap.
    - All staff must read and sign the 'Staff Code of Conduct' before using any school ICT resources.
    - The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
    - School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance
    - There will be regular reviews and audits of the safety and security of school ICT systems
    - Servers, wireless systems and cabling must be securely located and physical access restricted
    - All users will be provided with a username and password
    - Parents will be asked to sign and return a consent form.
    - Any persons not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.
    - The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network.

- The school will work with appropriate authorities to ensure systems to protect pupils are reviewed and improved.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2. Teaching and Learning:

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.
- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not, and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet for research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

3.Managing Internet Access

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the local authority.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details, or those of others, or arrange to meet anyone without specific permission.
- Staff or pupil personal contact information will not be published. The contact details given online will be that of the school office.
- Photographs and videos that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.
- Pupils full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published.
- Work can only be published with the permission of the pupil and parents/carers.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The appropriate use of learning platforms will be discussed and training given as its use develops.
- School leadership should be aware that technologies with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

4. E-Safety Communication and Complaints

- All staff will be given the school E-safety policy and its importance explained.
- E-safety rules will be posted in all rooms where computers are used, and discussed with pupils regularly.
- Staff and pupils will be informed that network and internet use will be monitored and appropriately followed up.
- A program of training in E-safety will be developed, based on material from CEOP.

- Parents' and carers' attention will be drawn to the school E-safety policy on the school web site.
- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences for pupils misusing the internet.

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

- The official school email service is regarded as safe and secure and is monitored Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

5. Data protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

6. Unsuitable / inappropriate activities

Some Internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

- child sexual abuse images
- promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gaming (educational)
- On-line gaming (non educational)
- On-line gambling
- On-line shopping / commerce
- File sharing
- Use of social networking sites
- Use of video broadcasting eg Youtube

Linked policies:

Appendix 1

Acceptable Use Policy – Staff

Covers use of digital technologies in school, including e-mail, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes.
- I will only use the approved, secure e-mail system for any school business. I will not browse, download or send materials that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate person.
- I will not allow unauthorised individuals to access email / internet / intranet / network of other school systems.
- I will not download any software or resources from the internet that can compromise the network, or are not adequately licensed.
- I understand that all internet usage can be logged.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not connect a computer, a laptop or other device to the network that does not have up-to-date anti-virus software.
- I will not use personal digital cameras or camera phones for transferring images of pupils or staff without permission.
- I will use the school learning platform in accordance with school policy.
- I will ensure that any private social networking sites that I create or contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities.
- I understand that the data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system will be kept private and confidential.
- I will ensure that I am aware of digital safeguarding issues and will embed them within my classroom practice.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.

I agree to abide by the school's Acceptable Use Policy.

Signature …… Date ……..

Full Name ……..

Job Title……

Appendix 2

E –SAFETY AGREMENT FORM

Internet Access

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

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

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

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

Parent / guardian signature: _____ Date:……