E-Safety Policy

2023-24

St Ambrose Catholic Academy is:

A member of St Joseph Catholic Multi Academy Trust

Transforming children's lives through a world-class Catholic education.

St Joseph Catholic Multi Academy Trust Registered in England as a company limited by guarantee number 13245781. Registered offices: Floor 3 Regus, No 1 Mann Island, Liverpool, L3 1BP

Electronic technologies are an essential part of 21st century life. This E-Safety Policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole. This policy will be displayed on the school website and should operate in conjunction with other school policies including;

- Safeguarding Policy
- Computing Policy
- Staff Code of Conduct

The E-Safety Policy will be reviewed annually by the coordinator and agreed by SLT using relevant guidance and has been formulated using guidance from LCC Acceptable Use Code of Practice.

Teaching and Learning

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-safety is therefore an essential part of the school's E-safety provision. Children and young people need the help and support of the school to recognise and avoid E-safety risks and build their resilience. **See appendix 1 – Appropriate Internet Use**

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages across each subject. The Computing curriculum includes an E-safety topic for each year group, which needs to be continually reinforced.

We continually strive to ensure:

- 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.
- That the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to deal with inappropriate information online or what to do when they feel threatened or uncomfortable.

- Pupils will be taught not to reveal personal details of themselves or others in e-mail or online communication, or arrange to meet anyone without specific permission.

Parents and Carers

Many parents and carers have only a limited understanding of E-safety risks and issues, yet play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimated how often children and young people come across potentially harmful and inappropriate material on the internet and through gaming and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through;

• Specific E-safety page on the school website
• Newsletters and letters
• Published Magazines (Eg; Vodafone magazine)
• Events and campaigns (Eg; Safer Internet Day)
• Parents training and courses

Radicalisation and Extremism

Pupils will be taught, through the curriculum, about the dangers of social media and the messages that they may find across the internet. We aim to help them recognise when they and others are at risk and equip them with the skills, strategies and language they need to take appropriate action. Staff will receive the relevant WRAP training to help identify when children may be at risk. Any concerns will be directed to the Safeguard Lead and appropriate action will be taken.

Managing Internet Access

Information System Security

• School ICT systems capacity and security will be reviewed regularly.
• Virus protection will be updated regularly.
• Security strategies will be discussed with Apex Network Solutions and other providers.

School Website (www.stambroseprimary.co.uk)

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
Pupils' full names will not be used anywhere on the website, particularly in association with photographs, which will be selected carefully. Written permission from parents or carers will be obtained for photographs of pupils to be published on the school website.

Social Networking and Personal Publishing

The school will block/filter access to social networking sites (excluding Twitter – see Social Media Policy). Pupils will be advised never to give out personal details of any kind, which may identify them or their location. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Any issues on Social Media, which impacts on school life, will be dealt with in by a member of Senior Leadership Team (See Positive Behaviour Policy). The use of such systems by teaching staff should be compatible only with their professional role **(User Code of Conduct for ICT – Appendix 2).**

Managing Filtering

The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. Some sites (such as Twitter and You Tube) will be unlocked for educational purposes but must be used appropriately and monitored by staff members **(Appropriate Internet use – Appendix 1).** In these circumstances, it will be highlighted to children that not everything will be appropriate or consistent with the ethos of our school. If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Co-ordinator or Safeguarding Lead where appropriate. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Video Conferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. Pupils should ask permission from the supervising teacher before making or answering a videoconference call **(Appropriate Internet use – Appendix 1)**.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Staff must use a school phone where contact with pupils is required.

Protecting Personal Data

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

Policy Decisions

Authorising Internet Access

All staff must read and sign the 'User Code of Conduct for ICT **(See Appendix 2)** before using any school ICT resource. At key stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Children will be asked to read and sign An Acceptable Use Agreement – this agreement will be discussed in detail to ensure children's **understanding (See appendix 3, 4 and 6).**

Assessing Risks

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer.

Neither the school nor Apex Network Solutions can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision on an ongoing basis to establish if the e-safety policy is adequate and that its implementation is effective. However, children will also be taught about e-safety risks, how to minimise these and dealing with them if they arise.

Handling E-Safety Complaints

Pupil Internet misuse will be dealt with by a senior member of staff. An incident form must be completed and handed to the Headteacher **(see appendix 5 – E safety Incident Log)** and will be dealt with in accordance with the Positive Behaviour Policy). Staff will be aware of expectations placed upon them through the Code of Conduct and 'Users Code of Conduct for ICT **(see appendix 2).** Any complaint about staff misuse must be referred to the head teacher. Complaints of a child protection nature must be dealt with in accordance with safeguarding procedures.

Unsuitable/Inappropriate Activities

School ICT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported and could lead to criminal prosecution.

Co-ordinator: J. Stinchcomb

Date of Policy: December 2023

Review Date: October 2024

Appendix 1: Acceptable Use

St Ambrose Catholic Academy

ICT/Internet Acceptable Use Policy/Guidelines

This document covers use of school digital technologies, networks etc. both in and out of school.

Access

- I will obtain the appropriate logon details and passwords from the ICT Coordinator.
- I will not reveal my password(s) to anyone other than the persons responsible for running and maintaining the system.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access school ICT systems or resources.

Appropriate Use

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'acceptable' or 'reasonable' by the Headteacher and Governing Body.
- I will never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues.
- This applies to any material of a violent, racist, homophobic, dangerous or inappropriate sexual content.
- I will not download, use or upload any material which is copyright, does not have the appropriate licensing or that might compromise the network.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the E - Safety coordinator or member of the SLT.

Professional Conduct

- I will not engage in any online activity that may compromise my professional responsibilities.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will never include pupils or former pupils as part of a non-professional social network or group.
- I will ensure that I represent the school in a professional and appropriate way when sending email, contributing to online discussion or posting to public websites.
- I will not browse, download or send material 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 school names contact (E-Safety lead or SLT member).

NOTE: The school system and use of the internet is monitored. Reports can be generated and sent to both the headteacher and Computing lead outlining any content accessed that may be inappropriate. The Computing

Lead will report straight to the Headteacher if there is any concern (unless it is the Headteacher themselves, in which case the lead will inform the Deputy Headteacher and they will collude and inform the chair of governors).

Personal Use

- I understand that I may use Internet facilities for personal use during my non-class based time (e.g. before school, lunch, breaks, etc. where PCs are available and not being used for professional/educational purposes).
- I understand that I may access private email accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.
- I understand that the forwarding of email chains, inappropriate 'jokes' and similar material is forbidden.
- I will not use the school Internet facilities for personal access to public discussion groups or bulletin boards, chat rooms or Instant Messaging.

Email

- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

Use of School equipment out of school

- I agree that any school equipment loaned to me is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue and Customs.
- I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software.
- I understand that any school equipment on loan can be tethered to my own log in credentials & that I must be aware of other content & its appropriateness. I must not link school equipment to other devices to prevent content being transferred between devices.

Social Networking

- I will ensure that my social networking accounts conform to the highest possible security & privacy settings.
- I will not be 'friends' with or make links with present or past pupils or parents unless I know them in a personal capacity.
- I will not bring the school's reputation into question through public criticism or comment on school business.
- I will display the highest standards of personal dignity on social networking sites.

Teaching and Learning

- I will always ensure suitable supervision of pupils that I have directed or allowed to use the Internet.
- I will embed the school's e-safety curriculum into my teaching, using agreed resources and materials.
- I will ensure I am aware of digital safeguarding issues so they are appropriately embedded in my classroom practice.
- I will only use the Internet for professional purposes when pupils are present.

Photographs and Video

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission
- I will never associate pupil names or personal information with images or videos published in school publications or on the Internet (in accordance with school policy and parental guidance).

Data protection

- I will not give out or share personal addresses (inc. email) or telephone contacts of any adult working at the school.
- I will not take pupil data, photographs or video from the school premises without the full permission of the Headteacher e.g. on a laptop, memory stick or any other removable media.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I will respect the privacy of other users' data, and will never enter the file areas of other staff without express permission.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

Copyright

- I will not publish or distribute work that is protected by copyright.
- I will encourage pupils to reference online resources/websites when they use them in report or publication.

User Signature

✓ I agree to abide by all the points above.

✓ I understand that it is my responsibility to ensure that I remain up-to-date and understand the school's most recent e-safety policies.

✓ I wish to be connected to the Internet via the school network and be able to use the school's ICT resources and systems.

Appendix 2: Pupil Acceptable Use Policy Agreement – Foundation Stage and Key Stage 1

This is how we stay safe when we use computers;

- I will ask a teacher or suitable adult if I want to use the computers.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult 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.

Child's name:……..

Signed:……

Date:……

Appendix 3 – Pupil Acceptable Use Policy Agreement – Key Stage 2

Internet use within school

I understand that I must use the school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
To do this;

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not download any software without permission.
- I will respect others' work and property and will not access, copy or remove any other users' files or work.
- I will immediately report any damages or faults involving equipment or software, however this may have happened.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- When I use the internet for research, I will take care to ensure the information is accurate.

Signed:……..

Pupil Name:…….

Date:……

Appendix 4: E-safety Incident log

E-Safety Incident Log

Please staple any printed evidence to support the incident

Date happened:

Time:

Name of Perpetrator (s):

Name of Victim(s);

Name and date of person reporting incident: If not reported, how was the incident identified? Include names of all adults to report (Eg; child, parent and staff member).

Where / how did the incident occur? (Texting, video call, website, blogging – please give specific site)

Description of incident: Please include type in incident (bullying, security risk, hacking, racism, sexual, illegal activities)

Action taken; Please include staff members involved in action, any referrals / safeguarding concerns, parental involvement, disciplinary action

Further action or outcomes: Please include continuous monitoring, CP file opened / added to, changes to e-safety policy or procedures required