Online Safety Policy
Local to St. Felix RC Primary School

Part of the Our Lady of Walsingham Catholic Multi Academy Trust

Prepared by	***Tracy Anderson*** *– Online Safety Lead*
Approved by the Committee/Governing body	*St. Felix Local Governing Body*
Signature of Chair of Governors	*Michael Bradshaw*
Date approved	*January 2021*
Review date	*January 2024*

Mission Statement

"As true followers of Jesus learning together, our school strives to be a community where everyone is valued, nurtured and encouraged to reach their full potential and where Christ's teaching guides responsible attitudes towards each other and the wider world."

TEACHING AND LEARNING

Why internet and digital communications are important

• The internet is an essential element in life for education, business, and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

• Internet use is part of the curriculum and a necessary tool for staff and pupils. The school internet access is provided by Suffolk County Council and includes filtering appropriate to the age of pupils. Any changes will be made in consultation with the Governing Body and the MAT.

• Pupils are taught correct internet use: what is acceptable and what is not. They are given clear objectives for internet use. See appendices: Pupils AUA.

• Pupils have supervised access to the computers and internet, during lessons and extra-curricular activities.
• Pupils are educated in the effective use of the internet via classroom Computing lesson, Online Safety in Computing and PHSE and through the Online Safety Team.

• Pupils are shown how to publish and present information appropriately to a wider audience including safe rules for publishing on social media and safe use of data.

Pupils will be taught how to evaluate internet content – appropriate to their age.
The school ensures that the use of internet derived materials by staff and by Pupils will comply with copyright law.

Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. They will be shown which sites to access; how to use the internet to research and not to copy and paste large chunks of the internet, to know that this is a copyright issue and plagiarises other's intellectual content.
Pupils are taught how to report inappropriate internet content through reporting systems.

The pupils are taught that visiting any websites and communicating online leaves a 'digital footprint'.

MANAGING INTERNET ACCESS

Information system security

• School ICT systems' security is reviewed regularly.

• Virus protection is updated regularly.

• Security strategies are monitored by Computing services team.

E-mail and other forms of e-communication

• Staff may only use approved e-mail accounts on the school system.

• Staff will monitor use of Microsoft Teams when allowing the use of chat or between pupil communication.

• Staff and pupils must not reveal personal details of themselves or others in electronic forms of communication, including social media, Microsoft Teams or in presentations of information.

• Staff to pupil communication may take place over Microsoft Teams regarding learning tasks set for homework or home learning.

Published content and the school website

• The only contact details published on the website are for the school (address, e-mail and telephone number). Staff or pupils' personal information is not published.

• The Head of School takes overall editorial responsibility and ensures that content is accurate and appropriate.

Publishing photographs, images, and work

• Photographs that include pupils are selected carefully and do not enable individual pupils to be clearly identified by name. The school aims to use group photographs rather than full-face photos of individual children.

• Pupils' full names are avoided on the school website or in communications between staff on e- mail. This is adhered to when teaching the pupils how to create blogs, vlogs or in presentation of information.

• Written permission from parents or carers is obtained before photographs or images of pupils are published and must be checked before use of said image. See appendix on Parental Permission.

• Parents receive information on image taking and publishing at the point of admission. This relates to school publications and outside publications, including use on the school website or on school social media. The choice made by the parents on Admission may be updated or changed by parents at the start of each year. These are noted in the confidential class information disseminated to each teacher at the start of the year and is maintained in the Confidential Class folder by the Administration team.

• The school controls and monitors access to social networking sites, and educates the pupils in their safe use.

• All users are advised never to give out personal details of any kind which may identify them, other people or their location.

• Pupils must not place personal photos on any social network space provided in the School.

• Pupils, parents and staff are advised on the safe use of social network spaces and the agreement on safe use is collected annually via Microsoft Forms.

Managing filtering

• The school works in partnership with Suffolk IT Services to ensure systems to protect pupils are reviewed and improved.

• If unsuitable content is passed by the school filtering system and seen by pupils, teachers must report this to the pupil's parents and report to Administration, to contact Suffolk IT services.

IT Services Manager / IT Technicians
In addition to their job description the IT Services Manager or IT Technician is responsible for ensuring:
• That the Academy's technical infrastructure is secure and is not open to misuse or malicious attack.
• That the Academy meets required online safety technical requirements and any relevant body's Online safety Policy / Guidance that may apply.
• Users may only access the networks and devices through a properly enforced password protection policy.
• The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
• That they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.
• That the use of the network, the internet, the Remote Learning Platform, remote access, and email is regularly monitored in order that any misuse or attempted misuse

can be reported to the Head of School or Online safety Coordinator for investigation, action, sanction, or support.

• That monitoring software / systems are implemented and updated as agreed in Academy policies.

Managing emerging technologies

• Emerging technologies will be examined for educational benefit: advice will be sought from Suffolk County Council and a risk assessment will be carried out before use in school is allowed. The risk assessment will be led by the MAT. Noted in parental permissions.

Other devices

• Pupil mobile phones are locked in safes at the start of each day. The only permitted mobile devices used in school are those owned by the school for teaching and learning purposes.
• The sending of abusive, offensive, or inappropriate material is forbidden.
• Children are not permitted to bring tablets or devices into school.

• Staff should not share personal telephone numbers with pupils or have pupils' numbers on their personal devices. Sharing personal telephone numbers with parents is not recommended. Staff make the decision to give out their number. Advice is given to staff to block access to their number if they are calling from personal devices.

Protecting personal data

• Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018 (GDPR)

Policy decisions authorising internet access

• All staff must read and accept the 'Staff Code of Conduct for ICT' via Microsoft Forms before using any school ICT resource. These are updated biannually with review of the Online Safety Policy or as and when a new member of staff joins St Felix, as part of their induction.

• The school Administration maintains a current record of all staff and pupils who are granted access to school ICT systems.

• Parents will be asked to read and confirm consent via Microsoft Forms to use the school's ICT systems.

• Pupils must agree to comply with the Acceptable Use Policy/Code of Conduct statement before being granted internet access. This information is maintained by

Administration and is contained in the confidential list of permissions in the Class Folder.
• Any person not directly employed by the school will be asked to sign the Acceptable Use Agreement form before being allowed to access the internet on the school site. This is part of the Onsite Visitor agreement kept by Administration.

ASSESSING RISKS

Inappropriate material

• The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Suffolk IT Services can accept liability for the material accessed, or any consequences of internet access. However, we would always inform parents of their child having been exposed to inappropriate material.

• The school will audit IT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective. The Academy is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of Academy data and personal protection of our Academy community very seriously. This means protecting the Academy network, as far as is practicably possible, against viruses, hackers and other external security threats.

The IT Manager or IT Technician will review the security of the Academy information systems and users regularly and virus protection software will be updated regularly. Any internet resources that staff sign up to for Academy purposes must be done using a Academy email account.
Students must not be granted access to any Academy or online resources via personal email accounts
Some safeguards that the Academy takes to secure our computer systems are: -
• Working toward a system to ensure that all personal data sent over the Internet is secure e.g., encrypted.

• Working toward a system so that staff are fully aware of their responsibility for ensuring that all personal data taken off site is secure.

Making sure that unapproved software is not downloaded to any Academy computers as any content may only be loaded with Administration rights.

Handling Online Safety complaints

• Complaints of internet misuse will be dealt with by the Online Safety Leader, who then reports this to the Designated Safeguarding Lead.

• Any complaint about staff misuse must be referred to the Head of School, or in the case where the complaint relates to the Head of School's misuse, this must be referred to the Chair of Governors.

• Complaints of a child protection nature must be referred to the Designated Safeguarding Lead and dealt with in accordance with school child protection procedures.

• Pupils and parents are informed of the complaints procedure and this is published on the school website.

• Pupils and parents are informed of consequences for pupils' misuse of the school computers or the internet.

Community use of the internet

• All use of the school internet connection by community and other organisations shall be in accordance with this policy.

COMMUNICATIONS POLICY

Introducing the Online Safety policy to pupils

Rules relating to the Academy code of conduct when online, and online safety guidelines, are to be displayed around the Academy.
Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, for example during RSE lessons and as part of the Computing curriculum, where personal safety, responsibility, and/or development are being discussed or taught. Discrete lessons are based on the materials provided by CEOP and Life to the Full.

• Pupils are informed that the network, Microsoft Teams, and internet use will be monitored.

• Any pupil misuse of ICT inside school and use of school ICT services will be discussed with parents. As use of Microsoft Teams is necessary for Homework and Home learning, sanctions to withdraw such provision cannot be made. However, it would be recommended that the pupil's use of Teams be closely monitored by both staff and parents.

Staff and the Online Safety policy

• All staff have access to the School Online Safety Policy.

• Staff are aware that internet traffic can be monitored and traced to the individual User.

• Staff who manage filtering systems or monitor ICT use are supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

• Parents and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school website.

• Parents and carers will be provided with additional information on Online safety from for the Online Safety Team (Year 5 pupils led by Online Safety leader)

• The school asks all new parents to consent to the Acceptable Use Agreement when their child is admitted to St Felix. See Appendices.

APPENDIX 1: LEGAL FRAMWORK SURROUNDING ONLINE SAFETY

This section is designed to inform users of legal issues relevant to the use of electronic communications. The law is developing rapidly

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 committed 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 someone else's password to access files);
• gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
• impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

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

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. 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 employment it belongs to the employer.

It is an infringement of copyright 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.

Data Protection Act 2018 This Act provides a comprehensive and modern framework for data protection in the UK, with stronger sanctions for malpractice.
It sets new standards for protecting general data, in accordance with the GDPR, giving people more control over use of their data, and providing them with new rights to move or delete personal data. Staff must be aware of the need for privacy and security of confidential data and cooperate with all existing systems in the school to ensure confidentiality of information
It preserves existing tailored exemptions that have worked well in the Data Protection Act 1998.

Education and Inspections Act 2006, sections 90 and 91
Provides statutory powers for staff to discipline pupils for inappropriate behaviour or for not following instructions, both on and off school premises. Section 94 also gives schools the power to confiscate items from pupils as a disciplinary penalty. These powers may be particularly important when dealing with online safety issues: online bullying may take place both inside and outside school, and this legislation gives schools the legal power to intervene should incidents occur. It also gives teachers the power to confiscate mobile phones, and other personal devices, if they suspect that they are being used to compromise the well-being and safety of others.

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 were to cause a recipient to suffer distress or anxiety.

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

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.

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 so to fear on each of those occasions.

Racial and Religious Hatred Act 2006
This Act makes it 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 abuse based on their race, nationality or ethnic background.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes 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
Permits 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.

Sexual Offences Act 2003
A 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) and then intentionally meet them or travel with intent 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. (Typically, teachers, social workers, health professionals, etc).

Any sexual intercourse with a child under the age of 13 commits the offence of rape. Schools should already have a copy of “Children & Families: Safer from Sexual Crime” document, which is available at the following website:
http://www.gmc-uk.org/sex_offences_act_2.pdf_48793788.pdf

APPENDIX 2: STAFF AGREEMENT

Staff, Governor and Visitor Acceptable Use Agreement - ICT Code of Conduct

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 adult users are aware of their responsibilities when using any form of ICT. All such users are expected to sign this policy and always adhere to its contents. Any concerns or clarification should be discussed with the Head of School.

• I appreciate that ICT includes a wide range of systems, including mobile phones, email, and social networking and that ICT use may also include personal ICT devices when used for school business.

• I understand that it is an offence to use a school ICT system and equipment for any purpose not permitted by its owner.

• I will not access personal accounts on school devices.

• I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

• I understand that I am responsible for all activity carried out under my username

• I will ensure that all school generated electronic communications are appropriate and compatible with my role.

• I will only use the approved, secure email system(s) for any school business

• I will ensure that all data is kept secure and is used appropriately and as authorised by the Head of School or Governing Body. If in doubt I will seek clarification. This includes taking data off site. For Cloud data storage and data sharing services e.g. Google, Microsoft 365, data or information stored on any cloud data storage must not be shared unless you are confident about how the system works, and who will be able to access the data.

• At school, I will not install any hardware or software without the permission of the subject leader for Computing.

• I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

• I will not use any form of Social Networking sites to post any comments about or pictures of other members of staff which could be interpreted as offensive, illegal or discriminatory.

• Images will only be taken, stored, and used for purposes in line with school policy and with written consent of the parent, carer, or adult subject. Images will not be distributed outside the school network or School Website, without the consent of the subject or of the parent/carer, and the permission of the Head of School

• I understand that my permitted 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 Head of School

• I will respect copyright and intellectual property rights.

• I will report any incidents of concern regarding children's safety to Head of School or other Senior Designated Professional.

Please Note -The Computer Misuse Act 1990 identifies three specific offences:
Unauthorised access to computer material (that is, a program or data).

• Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.

• Unauthorised modification of computer material
If the Computer Misuse Act 1990 is breached then a student or member of staff is likely to have the matter referred to other authorities including the police.
Online safety is a whole-Academy issue and responsibility.

User Signature

I agree to follow this Code of Conduct and to support the safe use of ICT throughout the school.

Name:……..….(printed)

Job title:……Date:……..

APPENDIX 3: EYFS / KS1 PUPIL AGREEMENT for Acceptable Use

This is how we stay safe when we use computers:

▪ I will ask a teacher if I want to use the computers, iPads, Interactive White Board, or other computing equipment.

- I will only use activities that a teacher has told or allowed me to use.
- I will take care of the computer and other computing equipment.
- I will ask for help from a teacher 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 or worries me on the screen.

- I know that I must be polite and take care with posting pictures or when I type something onto our Home learning page or class notebook.

- I will not meet other pupils on our Home Learning Platform without a school adult.
- I must keep my passwords private to me and my parents or carers. I must not share other's passwords.

Pupil _____ Date_____

Parent/ Carer _____

APPENDIX 4: KS2 PUPIL AGREEMENT for Acceptable Use.

These Online Safety Rules help to protect students and the school by describing acceptable computer use.

I know that the school rules apply to use of the internet.

I will only use ICT systems in school for learning tasks set by the teachers.
I will not post pictures or personal information of or about my family or friends on the internet without permission. I will not upload pictures of family or friends to Microsoft Teams.

I will store my learning in class folder. I will not access other's work or folders without their permission. I will show respect to others when using the Microsoft Teams chat for a learning task. I will not met other pupils on Teams without a school adult.

I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use in communication with others.

If I accidentally come across any material which is inappropriate, unpleasant or upsets me, I will report it to my teacher or teaching assistant immediately. I will not disseminate or save material that is inappropriate to other pupils.

I will not download or install software or files from any source, personal or otherwise, including memory sticks, on to school computers or other technologies, as this might cause viruses or other damaging problems which could infect the school system.

I will always respect the privacy and ownership of others' work on-line including copying others' writing or images to present as my own.

I understand the school may monitor, record, and control my use of the school's computer systems and online learning, via Microsoft Teams and, if necessary, report any misuse of the systems to other appropriate people.
I understand that these rules are designed to keep me safe and that accept that I will only be allowed to use the school equipment and systems by following the rules.

Pupil name:

Pupil signature: **Date:**

APPENDIX 5: PARENTAL FORM for Acceptable Use of Computing and Internet Services in Education Agreement

Parent / guardian name:……

Pupil name: …… Class: ……..

- As the parent or legal guardian of the above pupil(s), I grant permission for my child to have supervised access to use the internet, the Home Learning via Microsoft Teams and other IT facilities at school.
- I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Online Safety Policy/Code of Conduct. (OSP).
- I also understand that my son/daughter will be informed, as to the safety of new technologies or strategies.
- I know that the latest copy of the Online Safety Policy is available on the School Website for the Academy Trust.
- (http://www.stfelixhaverhill.com/), or from the school office, and that further advice about safe use of the internet can be found on the School Website or from the Computing Leader.
- 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 materials. These steps include using a filtered internet service, a monitored Home Learning platform and employing appropriate teaching practices and teaching online safety skills to pupils.
- I will not allow my child to bring in a mobile device, such as mobile phone or iPad or similar tablet device, to school without permission. If permission is granted, the device will then be stored securely during the school day. The school cannot accept any responsibility for any loss/damage that may occur. I understand that the school can check my child's computer files, mobile phone and the internet sites they visit.
- I understand that my child is not allowed to download or upload files at school from any source, including memory sticks, without permission, as these may contain unseen viruses or other damaging problems which could infect the school ICT system. I also know that the school may contact me if there are concerns about my son/daughter's online safety and online behaviour, including use of social media.
- 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 online safety.

Parent's signature:…… Date:……

APPENDIX 6: PARENTAL FORM - USE OF DIGITAL IMAGES

Use of digital images - photography and video (As recommended by Suffolk County Council)

To comply with the General Data Protection Regulations 2018, we need your permission before we can photograph or make recordings of your daughter / son.

We use the following rules for any external use of digital images: If the pupil is named, we avoid using their photograph. If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils' work, we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils are not referred to by name on the video, and that pupils' full names are not given in credits at the end of the film.

Only images of pupils in suitable dress are used. Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

• Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity, e.g., photographing children at work and then sharing the pictures on the interactive whiteboard or in the classroom allowing the children to see their work and make improvements.

• Your child's image for presentation purposes around the school, e.g., in school wall displays, presentations to capture images around the school or in the local area as part of a project or lesson.

• Your child's image being used in a presentation about the school and its work to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators, e.g. in a document sharing good practice; in our school prospectus, on the school website. In rare events, your child's image could appear in the media if a newspaper photographer or television film crew attend an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Use of digital images - photography and video:

I agree to the school using photographs of my child or including them in video material, as described in the above document 'Use of digital images – photography and video'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / guardian signature: …… Date: …….

APPENDIX 7: E-SAFETY INCIDENT REPORT LOG

Any breach of the e-safety agreement will be logged below and kept by the school

DATE	NAME	INCIDENT	ACTION TAKEN