St John Fisher Catholic Voluntary Academy

St Thomas Aquinas Catholic Multi-Academy Trust

E-safety Policy

Policy Date: 11/02/20			
Policy Review Date:	11/02/22	Anthony Gallagher	
Ratified by Governing Body:		Edward Hayes	E. J. Hayes.

Policy

1. Introduction

At St John Fisher Catholic Voluntary Academy, our mission is 'Aim High, work hard, be kind'.

We aim to achieve our mission by being inclusive, maintaining a safe and stimulating learning environment, securing outstanding learning and teaching, delivering our agreed curriculum, following Gospel values and working with parents, carers and the wider community.

We believe at the Academy that E-Safety both supports and strengthens what we aim to do in every aspect of Academy life. Our commitment to the welfare of our children and the upholding of our Safeguarding policy must be reflected through our implementation of the E-Safety policy.

2. Policy Scope

This policy applies to all members of the Academy community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the Academy computing systems, both in and out of the Academy.

The Education and Inspections Act 2006 empowers the Headteacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other E-Safety incidents covered by this policy, which may take place outside of the Academy, but are linked to membership of the Academy.

3. Policy Development

This E-Safety policy has been developed by Headteacher who is also the Computing Lead.

4. Policy Aims

The aim of this policy is to ensure that we safeguard our children against potential incidents of bullying, grooming, radicalisation or abuse through their use of technology. We aim to educate our children to use technology responsibly and safely, preventing them from either becoming victims of perpetrators of online abuse, whilst also treating equipment with respect and care. Through this policy, we aim to ensure that all members of the Academy community recognise and fulfil their shared commitment to E-Safety.

5. Equal Opportunities

St John Fisher Catholic Voluntary Academy is committed to equality of opportunity, and to promoting an ethos of dignity, courtesy and respect throughout the organisation.

Every effort will be made to ensure that a fair and consistent practice, as detailed in this policy and procedure, is carried out.

6. Quality Assurance

The quality of E-Safety delivery at St John Fisher Catholic Voluntary Academy will be assured by:

- Ensuring this policy is disseminated and adhered to.
- Monitoring the impact of the policy as set out in section 12.
- Addressing any underperformance in a timely manner, whether it has come to light through the monitoring procedures outlined in this policy or as a result of other Academy quality assurance mechanisms.

7. Roles and Responsibilities

The delivery of the E-Safety policy is a collective responsibility. The following section outlines the roles and responsibilities of individuals and groups within the Academy in relation to E-Safety.

7.1 The Governing Body

- There will be a designated Safeguarding Governor who will support the Academy and the Computing Leader in approving, monitoring and reviewing the effectiveness of the policy.
- The designated E-Safety Governor will review this policy on a biennial basis and support the Headteacher and Senior Leadership Team in their implementation of the policy through termly review meetings.
- The Governing Body will have access to online training on E-Safety via the National Online Safety website.

7.2 **The Headteacher and Senior Leaders**

- The Headteacher and (at least) another member of the Senior Leadership Team should be informed immediately in the event of an online safety allegation being made against a member of staff.
- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the Academy

community, though the day to day responsibility for online safety will be delegated to the Computing Leader.

- They will ensure that they keep up to date with statutory requirements and recommendations in relation to E-Safety.
- The Headteacher has overall responsibility for the data and data security.
- They will strive to provide suitable resources and training to support the aims of this policy.

The Computing Lead

The Computing Leader will promote an awareness and commitment to e-safeguarding throughout the Academy community.

They will take day-to-day responsibility for online safety issues and have a leading role in establishing and reviewing the Academy's E-Safety policy.

They will ensure that E-Safety is embedded across the curriculum.

The Computing Leader will ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

They will receive reports of online safety incidents via CPOMS and use the incident reports to inform future online safety developments.

They will communicate termly with the E-Safety Governor to discuss current issues and to review incident logs.

They will report half-termly to the Senior Leadership Team.

They will regularly research updates in E-Safety issues and legislation and know the potential for serious child protection issues that may arise from online misuse, including radicalisation.

The Computing Curriculum Leader will oversee the delivery of the E- Safety element of the Computing curriculum.

Technical Staff

The technical staff employed by St Thomas Aquinas Trust and/or St John Fisher will report any E-Safety related issues that arise to the Computing Leader.

They will ensure that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack.

They will ensure that the Academy meets required online safety technical requirements and any Trust E-Safety policy that may apply.

They will ensure that the Academy's web filtering policy is applied and updated on a regular basis.

They will ensure that all documentation relating to the Academy's e-security is up-to-date.

All Staff

All staff are responsible for ensuring that they have read, understood, signed and help promote the Staff, Governor and Volunteer Acceptable Use Agreement (see Appendix 1).

Teaching Staff

All teaching staff are responsible for ensuring that:

- online safety teaching is part of all computing lessons and is embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the E-Safety policy and all acceptable use policies.
- they monitor the use of digital technologies, mobile devices, cameras etc. in the Academy and implement current policies about these devices.
- they access and complete online training on E-Safety via the National Online Safety website.

Our Children

All of our children will be responsible for using the Academy's digital technology systems in accordance with the Pupil Acceptable Use Agreements (see Appendices 2 and 3).

Parents and Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.

They will have access to this policy and supportive materials concerning e-safety at home and these will be made available to them via the Academy's website.

Parents/carers should consult with the Academy if they have concerns about their child or other children's use of technology inside and outside of the Academy if related to their membership of the Academy.

They will support the Pupil Acceptable Use Agreements by signing the parent version.

Parents will have access to online training on E-Safety via the National Online Safety website.

Community Users and Volunteers

Community Users and volunteers who access Academy systems or the website as part of the wider Academy provision will be expected to read, understand, sign and help promote the Staff, Governor and Volunteer Acceptable Use Agreement (see Appendix 1).

Procedures

8 Time Allocation

The Academy has a commitment to ensure that all children in Years 1-6 have access to a Computing lesson for an hour a week. Within every Computing lesson, it is required that E-Safety is referred to. One lesson each half term is designated to the explicit teaching of E-Safety.

Every term, there will be an E-Safety assembly for the whole Academy but these may be delivered separately to each Key Stage (as appropriate) to ensure our children access age-appropriate content.

The Academy will participate in Safer Internet Day annually, with every child taking part in activities relating to E-Safety.

9 Planning

It is important that children are educated from an early age on how to safeguard themselves online. This doesn't just mean presenting them with information every now and then, it means embedding it into lessons across the curriculum, and facilitating discussion about it where possible.

E-Safety coverage will ensure that the expectations outlined in the Academy's objectives for Computing are met by each year group.

10 Teaching and Learning

The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the 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 in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught the importance of cross-checking information before accepting its accuracy.

Pupils will be taught how to be kind, when commenting online, using an app called Seesaw.

11 Assessment, Recording and Reporting

All incidents should be recorded using our safeguarding concern document and the correct people notified.

As soon as an incident is recorded, the Computing Leader should also be made aware, face to face, as a matter of urgency.
For cases of Cyber-bullying, please refer to the Anti-Bullying Policy.

12 Monitoring and Evaluation

The Governing body will be reported to by the Headteacher once a term via the Headteacher's report.

The Computing Leader will monitor the implementation of the policy by checking Safeguarding and behaviour logs for reported incidents, scrutinising Computing planning to check for coverage and carrying out staff and pupil questionnaires annually.

13 Review of the Policy

13.1 The Governing Body will review the E-Safety policy every two years.

13.2 The Governing Body will take account of the Headteacher's report in its review of the E-Safety policy.

Appendix 1

Staff and Governors Acceptable Use Agreement

By signing this agreement, you will have access to the school's systems and acknowledge that you agree to all the statements below. Additionally, that you have read and understand school policies which have a bearing on this agreement.

- I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care.

- I will educate children in my care in the safe use of digital technologies, acting on any online safety issues in accordance with the school's policies.

- I understand my use of the school's ICT systems/networks and internet are monitored.

- I recognise that whether within school or out of school, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to the school or impact on my role within the school and wider community.

- I know what GDPR is and how this has a bearing on how I access, share, store and create data.

- Any data that I have access to away from school premises must be kept secure and used with specific purpose. As outlined in the school's data protection policy, it is my responsibility to ensure when accessing data remotely that I take every bit of reasonable care to ensure the integrity and security of the data is maintained.

- I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role.

- I recognise that my social media activity can have a damaging impact on

  the school and children in my care at school if I fail to uphold my professional integrity at all times whilst using it.

- If I am contributing to the school's social media account(s) or website(s) I will follow all guidelines given to me, with particular care given to what images/video imagery and details can be uploaded.

- I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others' behaviours/conduct, I will notify the school at the earliest opportunity.

- I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others.

- I will never download or install software unless permission has been given by the appropriate contact at school.

- When using my own device- I will use with complete professionalism and in line with school policies.

…………………………………………………………………………………………

Staff / Governor/ Volunteer Name: ………………………………………………

Signed: ………………………………………………………

Date: ………………………………………………

Appendix 2

Pupil Acceptable Use Agreement

Foundation Stage and Key Stage One

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use a chrome book, a computer or a tablet.

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will not tell anyone my passwords.

I will only take photos, open files or follow links if I have been told to by a teacher.

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 or that is rude on the screen.

I will not write or send anything online that might upset someone.

I know that if I break the rules I might not be allowed to use a chrome book, computer or a tablet and my parent/carer may be told.

Appendix 3

Pupil Acceptable Use Agreement

Key Stage Two

This Acceptable Use Agreement is intended to ensure:
that I am responsible and stay safe when using the internet and other digital technologies at St John Fisher Catholic Voluntary Academy.
that I neither accidentally nor deliberately misuse the technologies at school.
that I have access to digital technologies at school, which can help me to learn.

This is the agreement that I will follow:

- I will only use ICT in school for school purposes.
- I will not use a personal device (phone, iPod, camera) in school. If I bring my phone or other device to school I will hand it in at the office for safe keeping until the end of the school day.
- I will not tell other people my passwords.
- I will only open/delete my own files unless I have permission from my teacher.
- I will not try to download or install programmes or software without permission
- I will not try to alter the settings of any digital technology unless I have permission to do so.
- I will report any damage or faults with the equipment or software.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- If I accidentally find anything that makes me upset or uncomfortable I will tell my teacher immediately.
- I must not give out my own details online, such as my name, school, phone number, or home address.
- I must never arrange to meet, try to call or make contact e.g. Facetime someone that I have met online by myself.
- I will not deliberately upload or add any images, video, sounds or text online or on a file that could upset any member of the school community.

- I will not use school's technology for on-line gaming, file sharing, internet shopping or video broadcasting (e.g. YouTube) unless I have permission of a member of staff to do so.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will not take or upload images of anyone without theirs and my teacher's permission.
- I will not open any attachments or hyperlinks in emails unless I know and trust the person/organisation who sent the email.
- I will not use or access social media sites.
- I know that my use of ICT can be checked and that my parent/carer will be contacted if school staff are concerned about my e-Safety.
- I understand that school can get involved and help to put right any incidents of inappropriate behaviour that I am involved in, which are covered by this agreement, out of school when they involve a member of the school community (e.g. cyber-bullying, use of images and personal information).

Acceptable Use Policy – Pupil Agreement

I have read and understand the Pupil Acceptable Use Agreement above and agree to follow these guidelines when:I use the Academy's systems and devices (both in and out of school).

I use my own devices in the Academy (when allowed) e.g. mobile phones, gaming devices, USB devices, cameras etc.

I use my own equipment out of the school / academy in a way that is related to me being a member of this Academy e.g. communicating with other members of the school, accessing school email, website etc.

Name of Pupil: ....

Class: ....

Signed: ....

Date: ....