# E-Safety Policy February 2017

## St John Fisher Catholic Voluntary Academy

**Mission Statement**

*This Mission Statement reflects the views of our pupils, staff and parents*

***'For I know the plans I have for you; plans to give you hope and a future.'*** Jeremiah 29:11

- I know that God made me and that he loves me very much.
- I want to grow in God's love and be the best that I can be.
- Every day I will get to know God better in prayer and meditation.
- I will always follow the academy rules because I know that they are there to help me and to make this a happy academy where children can learn.
- I will show care and respect for everyone I meet at all times.
- I will always try my best, even when I find things difficult.
- I will come to academy every day unless I am really too ill to attend.
- I will always tell the truth, even if I have done wrong.
- I will take care of the academy building, grounds and everything in it.
- My parents and everyone who works at Saint John Fisher will work together and always try their best to help me make the most of my God-given talents.

### The purpose of the e-safety policy

The purpose of this policy is to ensure that all staff, parents, Directors and children understand and agree the academy's approach to e-safety. The policy relates to other policies including ICT curriculum, Internet access, Bullying, Child Protection, Safeguarding and Health and Safety.

Health and Safety Policy  Behaviour Policy  Safeguarding and Child Protection Policy

### Writing and reviewing the e-safety policy

The academy will appoint an e-safety officer who will work closely with the Designated Child Protection officer.

The e-safety policy and its implementation will be renewed annually.

### Teaching and Learning

Why use of the Internet is important?

- The Internet is an essential element in 21st century life in education, business and social interaction. The academy has a duty of care to the pupils to provide 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.

**Internet use will enhance learning**

- The academy internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children.
- Pupils will be taught what internet use is appropriate 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

## Development

This e-safety policy has been developed by a working group / committee made up of:

- Headteacher: Mr Paul Ackers
- SLT: Jonathon Grattidge, Catherine Endsor, Paula Harlow
- E-Safety Officer: (E Sanger)
- Board of Directors

Consultation with the whole academy community has taken place through a range of formal and informal meetings.

## Schedule for Development / Monitoring / Review

| | |
|---|---|
| This e-safety policy was approved by the *Board of Directors* | ***Insert date*** |
| The implementation of this e-safety policy will be monitored by the: | *Headteachers, SLT, E-Safety Officer and the Board of Directors.* |
| Monitoring will take place at regular intervals: | *Annually* |
| The *Board of Directors* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals: | *Annually February 2018* |
| The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | *September 2018* |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | *Safeguarding Officer, Police, SLT and e-safety officer* |

The academy will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)

## Scope of the Policy

This policy applies to all members of the academy, volunteers, parents, visitors, who have access to and are users of academy ICT systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers the Headteacher to regulate the behaviour of students 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 is linked to membership of the academy.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of academy.

## Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the academy.

## Board of Directors

Directors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Directors receiving regular information about e-safety incidents and monitoring reports. The Directors have an E-Safety Director.

The role of the E-Safety Director will include:

- Meetings with the E-Safety Officer
- Monitoring of e-safety incident logs
- Monitoring of filtering
- Reporting to relevant committee meeting
- Attending relevant E-Safety training

### Headteacher

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the academy community, though the day to day responsibility for e-safety will be delegated to the E-Safety Officer.
- The Headteacher and SLT are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

### E-Safety Officer

- Will provide termly current e-safety lessons throughout the school to raise awareness
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the academy e-safety policies
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with the relevant body
- Liaises with academy's technical support team IDT
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- Meets regularly with E-Safety Director **Mr Cumpstone** to discuss current issues, review incident logs and filtering
- Sanctions will be the responsibility of the Headteacher, SLT and the e-safety officer

**Network Provider IDT**

Are responsible for ensuring that:

- **T**hat the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- That the academy meets required e-safety technical requirements
- That users only access the networks and devices through a properly enforced password protection
- The filtering system by the service provider is updated regularly
- That the use of the internet/email is regularly monitored in order that any misuse can be reported to the Headteacher, SLT and E-Safety Officer for investigation

**Teaching and Support Staff**

Are responsible for ensuring that:

- They have an up to date awareness of e-safety current practices
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Headteacher, SLT and E-Safety Officer for investigation
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official academy systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- All staff will take steps to prevent cyber-bullying.
- All staff monitor that pupils adhere to and follow the e-safety and acceptable use policies
- All staff monitor that the SMART rules are being adhered to
- All staff monitor that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- All staff where internet use is pre-planned for lessons, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

**Pupils**

- Are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Policy
- All children must follow the SMART rules stay safe system
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of academy and realise that the academy's E-Safety Policy covers their actions out of academy, if related to their membership of the academy

**Parents / 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. The academy will take every opportunity to help parents understand these issues through parents' e-safety evenings, newsletters, letters, website literature. Parents and carers will be encouraged to support the academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at academy events
- Access to parents' sections of the website
- Their children's personal devices in the academy (where this is allowed)

## Education –pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

## Education – parents / carers

The academy will raise parents and carers awareness of e-safety; the need to teach their children responsible use of the Internet and monitor what sites their children are using in order to ensure that they only access age appropriate social media.
The academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website
- Parents evenings, e-safety evenings
- High profile event e.g. Safer Internet Day

## Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out by the e-safety officer
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the academy e-safety policy and Acceptable Use Agreements)
- The E-Safety Officer will receive regular updates through attendance at external training events. E.g. Online safety live via UK Safer Internet Centre
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E-Safety Officer will provide advice / guidance / training to individuals as required.

## Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. These images should only be taken on academy equipment only and the personal equipment of staff should not be used for such purposes. See (Staff Acceptable Use Policy)
- Pupils must not take, use, share, publish or distribute images of others.
  See (Pupil Acceptable Use Agreement)
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the academy website or media outlets

## Data Protection

- 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 protected devices when they are using personal data.
- Transfer data using encryption and secure password

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted or password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device once it has been transferred or its use is complete

## Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the academy currently considers the benefit of using these technologies for education outweighs their risks.

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

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the Leadership team/e-safety officer – in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff, pupils or parents email, chat, must be professional in tone and content. These communications may only take place on official academy systems.
- EYEF/KS1/2 email addresses will be provided with individual academy email addresses for educational use.
- Any staff member communicating with pupils must use academy email and must always copy in the Leadership team.
- Pupil's should be taught about e-safety issues, such as the risks attached to the sharing of personal details.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

## Social Media - Protecting Professional Identity

Expectations for teachers' professional conduct are set out in 'Teachers Standards 2015'. Ofsted's e-safety framework updated 2016 reviews how online safety is now included in Ofsted's safeguarding documentation.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education.pdf Annex C page 62

All academies have a duty of care to provide a safe learning environment for pupils and staff. Academies could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the academy through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

**Academy staff should ensure that:**

- No reference should be made in social media to pupils, parents / carers or academy staff
- They do not engage in online discussion on personal matters relating to members of the academy community
- Personal opinions should not be attributed to the academy

## Protecting children from the risk of radicalisation (PREVENT)

Is seen as part of schools' wider safeguarding duties, and is similar in nature to protecting children from other harms (e.g. drugs, gangs, neglect, sexual exploitation), whether these come from within their family or are the product of outside influences. The school is aware of the increased risk of online radicalisation, as terrorist organisations such as ISIL seek to radicalise young people through the use of social media and the internet. This is managed as part of this e-safety policy, linked with the safeguarding policy. Safeguarding Policy

## Unsuitable / inappropriate activities

The academy believes that pupils and staff must not engage in unsuitable or inappropriate activities in an academy context and that users should not engage in these activities in academy or outside academy when using academy equipment or systems.

## Responding to incidents of misuse

If a pupil suspects unsuitable or inappropriate activities are taking place they must inform their class teacher/staff. If a member of staff suspects unsuitable or inappropriate activities are taking place they must inform the Leadership team immediately. This guidance is intended for staff to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

### Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, the Leadership team must be informed so that the police and CEOP can be informed appropriately.

### Other Incidents

All members of the academy community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

### In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Police involvement and/or action
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material

- Other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

## Academy Actions & Sanctions

It is more likely that the academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the academy community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

## Academy Policy

Digital technologies have become integral to the lives of children and young people, both within academy and outside academy. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The academy will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users

See (Pupil Acceptable Use of ICT)

Date: To be reviewed by February 2018

Chair of Directors Signature: