Faith Primary Academy

Online Safety Policy

Our school vision is inspired by the bible verse Ephesians 5: 8-9:
For you were once darkness, but now you are light in the Lord. Live as children of light.

Faith Primary is a joint Catholic and Church of England Academy. Guided by our Christian ethos we are here to serve the community, helping the children and all involved in the school to reach their full potential in a safe and happy environment.

"Loving and Learning in the Light of the Lord"

Love Generosity Compassion Courage Forgiveness Friendship Respect

Reviewed: **September 2025** Review date: **September 2027**

Online Safety Policy

Introduction

This online safety policy recognises the commitment of Faith Primary Academy in keeping staff and pupils safe online and acknowledges its part in the school's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole school community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The online safety policy supports this by identifying the risks and the steps we are taking to avoid them. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

• Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

• Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying;
And

• Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group.
(DfE Keeping Children Safe in Education 2025)

This policy shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. We wish to ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken. We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with pupils.

Our expectations for responsible and appropriate conduct are set out in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to online safety, we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets from loss or inappropriate use.

The scope of this policy

This policy applies to the whole school community including the Senior Leadership Team (SLT), Governing Body (GB), all staff employed directly or indirectly by the school, volunteers, visitors and all pupils.

The Senior Leadership Team and school governors will ensure that any relevant or new legislation that may impact upon the provision for online safety within school will be reflected within this policy.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate online behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the *school*:

Governors
Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. Termly safeguarding visits to school will take place by the Safeguarding Governor and their role will include:

- regular meetings with the Online Safety Lead as part of Safeguarding monitoring
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors/Board/Committee/meeting

Headteacher and Senior Leaders

- The *Headteacher* has a duty of care for ensuring the safety (including online safety) of members of the school community and is also the *Online Safety Lead*.
- The Headteacher and SLT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority relevant body* disciplinary procedures).
- *The Headteacher is the Online Safety Lead and undertakes relevant training to undertake the role and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.*
- *The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The teaching team will receive termly monitoring reports from the Online Safety Lead.*

Online Safety Lead
The Online Safety Lead is Miss Fox (Head of School and DSL)

• takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
• ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
• provides training and advice for staff
• liaises with school technical staff
• receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
• meets regularly with Safeguarding Governor to discuss current issues, review incident logs
• attends relevant meetings of *Governors*
• reports regularly to the teaching team

Any incidents that occur and the investigation, actions and sanctions will be the responsibility of the Headteacher or the Designated (or deputy) Safeguarding Lead.

Teaching and Support Staff

Are responsible for ensuring that:
• they have an up-to-date awareness of online safety matters and of the current *school* online safety policy and practices
• they have read, understood and signed the staff acceptable use agreement
• they report any suspected misuse or problem to the *Headteacher/ Online Safety Lead* for investigation/action/sanction
• all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
• online safety issues are embedded in all aspects of the curriculum and other activities
• pupils understand and follow the Online Safety Policy and acceptable use policies
• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
• in lessons where internet use is pre-planned 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

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:
• sharing of personal data
• access to illegal/inappropriate materials
• inappropriate on-line contact with adults/strangers
• potential or actual incidents of grooming
• online-bullying

(N.B. it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.)

Students/Pupils:

• are responsible for using the *school* digital technology systems in accordance with the pupil acceptable use agreement
• 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 online bullying.
• should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's* online safety policy covers their actions out of school, if related to their membership of the school

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 *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature.* Parents and carers will be encouraged to support the *school* in promoting good online safety practice and to follow guidelines on the appropriate use of:
• digital and video images taken at school events

We believe it is important to help all our parents and carers develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will offer opportunities for finding out more information through meetings, the school newsletter and website.

We will ask all parents to discuss the pupil's Acceptable Use Policy with their child and return a signed copy to the school. We also ask parents to sign the home school agreement which includes a statement about their use of social networks in situations where it could reflect on our school's reputation and on individuals within the school community.

Policy Statements

Education –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 online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
• A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
• Key online safety messages should be reinforced as part of a planned programme of assemblies and 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
• Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015, which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
• Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
• 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 students/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.
• Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
• It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Within our school curriculum, online safety is taught explicitly within our Computing curriculum as well as taught through PSHE and through focus days such as Safer Internet Day each February and our whole school safety week in the summer term each year.
Education – Parents/carers
Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The school will therefore seek to provide information and awareness to parents and carers through:
• Curriculum activities
• Letters, newsletters, web site,
• *Dedicated Online Safety materials for Parents/Carers*
• High profile events/campaigns e.g. Safer Internet Day

Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
• A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
• All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school/academy online safety policy and acceptable use agreements.
• *It is expected that some staff will identify online safety as a training need within the performance management process.*

• This online safety policy and its updates will be presented to and discussed by staff in staff meetings/training sessions.
• The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Training – Governors
Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This training will be provided either by the Trust Safeguarding Lead or via the National College.

Acceptable Use Policies
School has a number of AUPs for different groups of users. These are shared with all users yearly and staff and pupils will be expected to agree to them and follow their guidelines. We will ensure that external groups and visitors to school who use our ICT facilities are made aware of the appropriate AUP.

School Acceptable Use Policy documents

- School staff Acceptable Use Policy- Equipment, Software and Services (Code of Conduct)
- Parents and Pupils Acceptable Use Policy (Home School Agreement)
- Terms and Conditions for Internet and Wi-Fi- Visitors and Guests

Teaching and Learning

We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present. We deliver a planned and progressive scheme of work to teach online safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity.

Online safety is taught in specific Computing and PSHE/RSHE lessons and also embedded across the curriculum, with pupils being given regular opportunities to apply their skills. We teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

We discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons. We will remind pupils about the responsibilities to which they have agreed through the AUP. Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies

Monitoring

In order to be compliant with the Prevent Duty and Keeping Children Safe in Education 2024, the school will:

• Use the findings of the annual Prevent risk assessment to put appropriate internet and network monitoring systems in place.

• Pupils are always supervised by staff while using the internet as this reduces the risk of exposure to extremist, illegal or inappropriate material; direct supervision also enables school staff to take swift action should such material be accessed either accidentally or deliberately.

• Internet and network use is monitored continually by the school technician to identify access to websites or internet searches which are a cause for concern.

• Senso network monitoring software is used throughout school. This is monitored and provides reports of inappropriate communications, searches and website access. Any cause for concern is reported to the DSL and Online Safety Lead.

Access to school systems

The school decides which users should and should not have internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their role in school. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to school systems is covered by specific agreements and is never allowed to unauthorised third party users

Using the internet

We provide the internet to

• Support teaching, learning and curriculum development in all subjects

• Support the professional work of staff as an essential professional tool

• Enhance the school's management information and business administration systems

• Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

All users of the school IT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,

Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

Using email

Email is regarded as an essential means of communication and the school provides all members of staff with an email account for school-based communication. Communication by email between staff and parents will only be made using the school email account and should be professional and related to school matters only. Email messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. There are systems in place for storing relevant electronic communications which take place between school and parents.

- Use of the school email system is monitored and checked.
- It is the personal responsibility of the email account holder to keep their password secure.
- As part of the curriculum pupils are taught about safe and appropriate use of email.
- Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email address.
- Responsible use of personal web mail accounts on school systems is permitted outside teaching hours.

Using Seesaw

Seesaw is used as an essential means of communication and the school provides all members of teaching staff with a login for school-based communication. Communication by Seesaw message between staff and parents will only be made using the school Seesaw account and should be professional and related to school matters only. Seesaw messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. There are systems in place for storing relevant electronic communications which take place between school and parents.

- Use of Seesaw is monitored and checked.
- It is the personal responsibility of the account holder to keep their password secure.
- Under no circumstances will staff contact pupils, parents or conduct any school business using a personal Seesaw account.

Publishing content online
E.g. using the school website, learning platform, blogs, wikis, podcasts, social network sites, livestreaming
School website:

The school maintains editorial responsibility for any school initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, email and telephone number. Contact details for staff published are school provided. Identities of pupils are protected at all times and school obtains permission from parents for the use of pupils' photographs (Home School Agreement) . Group photographs do not have a name list attached.

Creating online content as part of the curriculum:

As part of the curriculum we encourage pupils to create online content. Pupils are taught safe and responsible behaviour in the creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents or younger children. Personal publishing of online content is taught via age-appropriate sites that are suitable for educational purposes. They are moderated by the school where possible. Pupils will only be allowed to post or create content on sites where members of the public have access when this is part of a school related activity. Appropriate procedures to protect the identity of pupils will be followed.

- We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Online material published outside the school:

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school. Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multimedia and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

We ask all parents/carers to sign an agreement about taking and publishing photographs and video of their children (in publications and on websites) and this list is checked whenever an activity is being photographed or filmed.

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

We are happy for parents to take photographs of their own children at school events but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own they should not be uploaded to social media sites.

Using video conferencing, web cameras and online meeting apps

We may use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. We ensure that staff and pupils take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff. Pupils do not operate video conferencing equipment, answer calls or set up meetings without permission from the supervising member of staff.

Video conferencing equipment is switched off and secured when not in use and online meeting rooms are closed and logged off when not in use.

All participants are made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

Using mobile phones

Personal mobile devices belonging to pupils including mobile phones are permitted on school premises but must not be used within school hours. Personal devices are brought onto school premises by pupils at their own risk. The school does not accept liability for loss or damage of personal devices.

During lesson time we expect all mobile phones belonging to staff to be stored in a secure location unless there is a specific agreement for this not to be the case.

Where required for safety reasons in off-site activities, a school mobile phone is provided for staff for contact with pupils, parents or the school. Staff will never use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.

Unauthorized or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request. If the victim is another pupil or staff member we do not consider it a defence that the activity took place outside school hours.

The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress is online bullying; this will be considered a disciplinary matter.

We make it clear to staff, pupils and parents that the Headteacher has the right to examine content on a mobile phone or other personal device to establish if a breach of discipline has occurred.

Using wearable technology

Wearable technology includes electronic fitness trackers and internet enabled 'smart' watches. Wearable technology is permitted on school premises but must not be used within school hours.

Personal devices are brought onto school premises by pupils at their own risk. These devices must be handed to the class teacher on the arrival to school. The school does not accept liability for loss or damage of personal devices.

Using mobile devices

We recognise that the multimedia and communication facilities provided by mobile devices (e.g. iPad, iPod, tablet, netbook, Smart phones) can provide beneficial opportunities for pupils. However their use in lesson time will be with permission from the teacher and within clearly defined boundaries.
Pupils are taught to use them responsibly.

Using other technologies

As a school we will keep abreast of new technologies and evaluate both the benefits for learning and teaching and the risks from an online safety point of view.

We will regularly review the online safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

Protecting school data and information

School recognises the obligation to safeguard staff and pupils' sensitive and personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation

Pupils are taught about the need to protect their own personal data as part of their online safety awareness and the risks resulting from giving this away to third parties.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:
• Staff are provided with secure cloud storage for storing sensitive data
• All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended
• Staff are provided with appropriate levels of access to the school management information system holding pupil data. Passwords are not shared and administrator passwords are kept securely
• Staff are aware of their obligation to keep sensitive data secure when working on computers outside school

• All devices taken off site, e.g. laptops, tablets, removable media or phones, are secured to protect sensitive and personal data and not left in cars or insecure locations.
• When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
• Remote access to computers is by authorized personnel only

Management of assets

Details of all school-owned hardware and software are recorded in an inventory.

All redundant IT equipment is disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2013.

Responding to online safety incidents

- All online safety incidents are recorded onto CPOMS and reported to Governors.
- Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.
- In situations where a member of staff is made aware of a serious online safety incident concerning pupils or staff, they will inform the DSL, online safety lead, their line manager or the headteacher who will then respond in the most appropriate manner.
- Instances of online bullying will be taken very seriously by the school and dealt with using the school's anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim. Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's online safety lead and technical support and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.
- School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about child protection or the discovery of indecent images on the computer, then the procedures outlined in school's Safeguarding policy will be followed.

Dealing with complaints and breaches of conduct by pupils:
• Any complaints or breaches of conduct will be dealt with promptly
• Responsibility for handling serious incidents will be given to the DSL and a senior member of staff

• Parents and the pupil will work in partnership with staff to resolve any issues arising • Restorative practice will be used to support the victims
• There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies The following activities constitute behaviour which we would always consider unacceptable (and possibly illegal):
• accessing inappropriate or illegal content deliberately
• deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, in breach of the Equalities Act or violent/threatening violence
• online peer on peer abuse and sexual harassment
• continuing to send or post material regarded as harassment or of a bullying nature after being warned
• staff using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites) The following activities are likely to result in disciplinary action:
• any online activity by a member of the school community which is likely to adversely impact on the reputation of the school
• accessing inappropriate or illegal content accidentally and failing to report this
• inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons
• sharing files which are not legitimately obtained e.g. music files from a file sharing site
• using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute
• attempting to circumvent school filtering, monitoring or other security systems
• circulation of commercial, advertising or 'chain' emails or messages
• revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
• using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)
• transferring sensitive data insecurely or infringing the conditions of the Data Protection Act 2018 The following activities would normally be unacceptable; in some circumstances they may be allowed e.g. as part of planned curriculum activity or by a system administrator to problem solve
• accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
• sharing a username and password with others or allowing another person to log in using your account
• accessing school ICT systems with someone else's username and password
• deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

Online safety

Online safety Online Safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.
• Online Safety concerns safeguarding children and young people in the digital world.
• Online Safety emphasises learning to understand and use new technologies in a positive way.
• Online Safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
• Online Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

An important step in improving online safety at school is identifying what the potential risks might be. KCSIE groups online safety risks into four areas: content, contact, conduct and commerce (sometimes referred to as contract).2 These are known as the 4 Cs of online safety.

Content

Content is anything posted online – it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

Conduct

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm – for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

Commerce

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.

At Faith Primary Academy we ensure that children are safe and responsible on line by ensuring that:

- Pupils are supervised appropriately when they use the Internet.
- Pupils are given clear objectives for Internet use.
- Pupils are provided with lists of relevant and suitable web sites.
- Pupils are aware of their responsibilities.
- Parents and carers are aware of their responsibilities in relation to child safety on the internet.
- Curriculum planning identifies opportunities to enrich and extend learning activities via access to the Internet
- Strong effective filtering and monitoring systems are in place
- Internet access is overseen by All Saints Multi-Academy Trust which provides a firewall that filters out inappropriate sites
- We work with All Saints Multi-Academy trust's ICT department to ensure systems to protect pupils are regularly reviewed and improved.

Reviewing online safety

An annual review of online safety policy and practice will be carried out with the support of All Saints Academy Trust.