

E-Safety Policy









Organisation	The Saints Federation				
Title	E-Safety Policy				
Author	School/Governing Body				
Owner	Head teacher and Governing body				
Protective marking	NOT PROTECTIVELY MARKED				
Review date:	Every Three years or sooner if needed				

Revision history

Revision Date	Revision	Previous version	Description of revision
December 2018	1.0	N/A	Policy created and signed off
November 2019			Annual Review
December 2020			Review

Signed by Chair of Governors on behalf of the Governing Body:
Signed by the Head Teacher:
Date approved: (by full Governing Body)
Date of review:

As a rights respecting school we aim to ensure all children, staff and families are aware of children's rights. We aim to not only teach about children's rights but also model rights and respect in all relationships. This policy is linked to Articles 13, 15, 16, 17, 36 (UNCRC)

<u>Introductio</u>n

Use of exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the improper or unsafe use of technology can present challenges to children, young people, volunteers and staff. The aim of this policy is to ensure a consistent approach across the school to minimising risk and educating children and staff in matters relating to the safe use of the IT and the internet.

Some of the potential risks could include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to exploitation and abused by those with whom they make contact on the internet.
- · The sharing / distribution of personal images without an individual's consent or knowledge
 - Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Blackmail involving threats to life, dignity and violence.
- Poor or inappropriate supervision of Internet access leading to the viewing of harmful or inappropriate.
- · Risk of sexual exploitation

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, antibullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Monitoring and Review of the Policy

The implementation of the policy will be monitored by <u>The E-Safety Co-ordinator and school</u> SLT

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.

Should serious e-safety incidents take place, the following external persons / agencies should be informed: <u>LA Schools ICT Strategic Manager, LA Safeguarding Officer, Police</u>

Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of o students / pupils (e.g. CEOP ThinkUknow survey) o parents / carers o staff

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

The Education and Inspections Act 2006 empowers Executive Executive Headteachers, to such extent as is reasonable, to regulate the behaviour of students / 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 cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regards to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published behaviour policy.

The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate esafety behaviour that takes place out of school.

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors 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 Governors regular information about e-safety incidents and monitoring reports. A named governor has taken on the role of *E-Safety Governor*.

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- · regular monitoring of e-safety incident logs
- reporting to relevant Governors meetings

Executive Executive Headteacher and Senior Management Team:

- The Executive e Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator
- The Executive Headteacher / SLT are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Executive Headteacher / SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Coordinator.

E-Safety Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy.
- 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 including how to be alert to the potential misuse of digital media and take responsibility for reporting it appropriately
- · liaises with the Local Authority.
- · liaises with ICT technical staff.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- · meets regularly with E-Safety Governor to discuss current issues and review incident logs.
- attends relevant meeting of Governors
- reports regularly to Senior Management Team.

Teaching and Support Staff are

responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safety Co-ordinator /Executive Headteacher for investigation / action / sanction.
- all digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- · e-safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- students / 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 lesson and other school activities (where allowed) and implement current policies about these devices.
- in lessons where internet use is pre-planned 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

Designated person for child protection / Child Protection Officer

Should be trained in e-safety issues and be aware of the potential for serious child protection 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
- cyber-bullying

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of safe use of digital media and how to report abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand school policies on the use of mobile phones, digital
 cameras and hand-held devices. They should also know and understand school 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 school and realise that the school's E-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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website information and local e-safety literature.

Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website.
- digital media and how to report abuse, misuse or access to inappropriate materials

Visiting Adults and Pupils

Users who access school ICT systems / website / VLE via login as part of the Extended School provision will be expected to sign an AUP before being provided with access to school systems.

Education – students / pupils

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

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.
- 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 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 can 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.
- Students should be supported to understand and report unsafe or harmful digital misuse.

Education – parents / carers

Many parents and carers have only a limited understanding of e-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 on-line 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 messages,
- Parents / Carers evenings / sessions
- Reference to the relevant web sites / publications

Education – The Wider Community

The school / academy will provide opportunities for local community groups / members of the community to gain from the school's / academy's e-safety knowledge and experience. This may be offered through the following:

- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide e-safety information for the wider community

Cyberbullying

Cyber bullying has become an increasing concern for schools, parents and children alike. Cyber bullying has traditionally been defined as harassment and victimisation using interactive technology. It is important that we understand the complex nature of cyber bullying to be able to prevent incidents and respond effectively to incidents when they arise. For example, one comment made online becomes bullying when it is repeatedly forwarded or commented on by others, which in turn is seen by multiple people over a sustained period. It can often be difficult to gain closure when subject to a cyberbullying incident when the comment or photo can resurface at any time.

Cyber bullying differs from traditional forms of bullying and can have a significant detrimental impact upon individuals who are targeted by such behaviour. The 24/7 nature of cyber bullying can make it difficult for a target to escape the attacks directed at them. In some cases, an individual may not know they are being bullied if they have not seen the content posted about them, but it is important to understand that the intentions of the perpetrator is still to bully the individual in question by posting humiliating and hurtful content.

We promote the positive use of Interactive Technology and Social Media, where pupils are provided with opportunities to discover the benefits social media has to their learning and social development. We understand that it can sometimes be easy to forget that we are talking to real people with real emotions when using social media; as such we encourage and promote responsible use and respectful communications with others online.

All incidents of inappropriate use of social media are taken seriously and we encourage all members of the school community to report any incidents of inappropriate use of social media and interactive technology.

Inappropriate use of social media includes, but not restricted to:

- harassment and intimidation of others,
- · sending hateful messages,
- posting inappropriate and unwanted pictures online and;
- creating content which has the potential to hurt, embarrass and humiliate others.
- Online exploitation including sexual abuse

We respond to inappropriate use and bullying online in accordance with the procedures and guidance outlined in our anti-bullying and behaviour policy. Support is provided to all parties involved in incidents of bullying online and parents will be notified following a report of bullying online. Where appropriate we will contact external agencies to obtain further advice, information and provide additional support to individuals if necessary. Restorative approaches

will be implemented to resolve any issues of inappropriate use of social media. We understand that in some circumstances there will be a requirement to involve the police. We will liaise with our Police School Liaison Officer for advice on the appropriate route and action to take in these circumstances.

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. An audit of
 the e-safety training needs of all staff will be carried out regularly. It is expected that some
 staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator will receive regular updates through attendance at Consortium training sessions and by reviewing guidance documents released by BECTA / Consortium / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

<u>Training – Governors</u>

Governors should take part in e-safety training / awareness sessions, with importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Use of digital and video images - Photographic, Video

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. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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 school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Schools are advised to ensure that policies on the storage and destruction of images are in place
- Care should be taken when taking digital / video images that pupils are appropriately
 dressed and are not participating in activities that might bring the individuals or the school
 into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- 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 in association with photograph, unless enhanced signed consent has been given.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Communications

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

	Staff	& oth	er adu	ılts	Stude	ents /	Pupils	•
Communication Technologies	Allowed	Allowed at certain times / places	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times / places	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	Х						Х	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on personal mobile phones or other camera devices				X				X
Use of other mobile devices eg tablets, gaming devices			Х					X
Use of personal email addresses in school, or on school network		Х						X
Use of school email for personal emails				X				X
Use of chat rooms / facilities				X				X
Use of instant messaging/messaging apps				X				X
Use of social networking sites				X				X
Use of blogs		Х					Х	

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or					
pass on, material, remarks, proposals or comments that contain or relate to:	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.				
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008				
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986				
	pornography				X
	promotion of any kind of discrimination				X
	threatening behaviour, including promotion of physical violence or mental harm				X
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X
Using school systems to run a private	vate business				X
Using systems, applications, web safeguards employed by the scho	sites or other mechanisms that bypass the filtering or other ool / academy				Х
Infringing copyright					Х
	ential or proprietary information (eg financial / personal / network access codes and passwords)				X
Creating or propagating computer				Х	
Unfair usage (downloading / uple internet)	oading large files that hinders others in their use of the				Х
On-line gaming (educational)			Х		
On-line gaming (non educational)					Х

On-line gambling			X
On-line shopping / commerce			X
File sharing		Х	
Use of social media			X
Use of messaging apps			X
Use of video broadcasting egYoutube		Х	

Social Media - Protecting Professional Identity

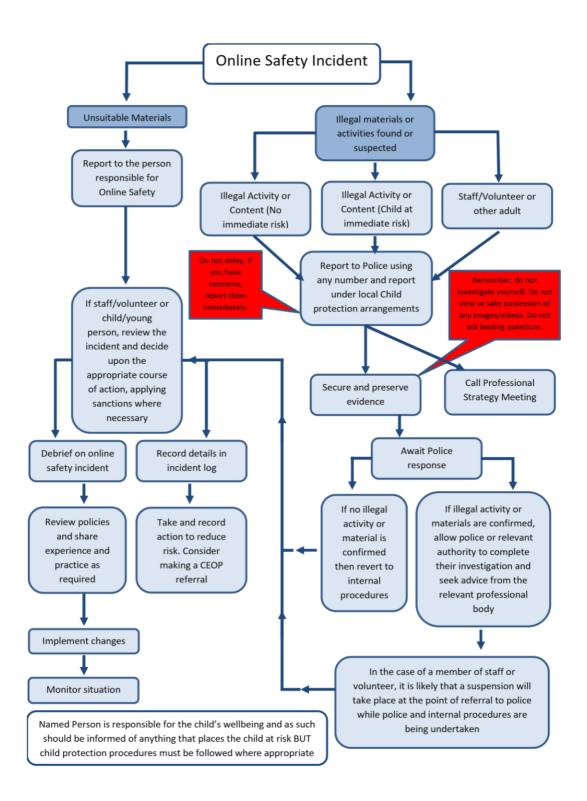
All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully,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

- The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school 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
 Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the Senior Leadership Team to ensure compliance with all other school policies.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the "Guidance for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found in the appendix.

It is more likely that the school 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 school 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 that follows. Please refer also to the school's Data Protection Policy and Publication Scheme.

Deliberately accessing or trying to access material that could be considered lilegal (see list in earlier section on unsuitable / inappropriate activities). Unauthorised use of non-educational sites with the control of the control	Pupiis	Actions	, Oa	ilotioi	13					
material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). Unauthorised use of non-educational sites X during lessons Unauthorised use of mobile phone / digital X X X X	Incidents:		Refer to SMT	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg exclusion
Unauthorised use of mobile phone / digital X X X X			X	X	X	X	X			
Unauthorised use of social networking / X	Unauthorised use of non-educational sites during lessons	X								
Unauthorised downloading or uploading of files X X X Allowing others to access school network by sharing username and passwords Attempting to access or accessing the school network, using another student's / pupil's account Attempting to access or accessing the school network, using another student's / pupil's account Attempting to access or accessing the school network, using the account of a member of staff Corrupting or destroying the data of other users X X X Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature Continued infringements of the above, following previous warnings or sanctions Actions which could bring the school into disrepute or breach the integrity of the ethos of the school Using proxy sites or other means to subvert the school's filtering system Accidentally accessing offensive or pornographic material and failing to report the incident Deliberately accessing or trying to access offensive or pornographic material that infringes the ecopyright of another person or infringes the	Unauthorised use of mobile phone / digital camera / other handheld device	X	X	X						
Allowing others to access school network by sharing username and passwords Attempting to access or accessing the school network, using another student's / pupil's account Attempting to access or accessing the school network, using the account of a member of staff Corrupting or destroying the data of other users X X X Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature Continued infringements of the above, following previous warnings or sanctions Actions which could bring the school into disrepute or breach the integrity of the ethos of the school Using proxy sites or other means to subvert the school's filtering system Accidentally accessing offensive or pornographic material and failing to report the incident Deliberately accessing or trying to access offensive or pornographic material that infringes the copyright of another person or infringes the	Unauthorised use of social networking / messaging apps / personal email	X	X	X						
Attempting to access or accessing the school network, using another student's / pupil's account Attempting to access or accessing the school network, using another student's / pupil's account Attempting to access or accessing the school network, using the account of a member of staff Corrupting or destroying the data of other users X X X X X X X X X X X X X X X X X X X	Unauthorised downloading or uploading of files		X	X						
network, using another student's / pupil's account Attempting to access or accessing the school network, using the account of a member of staff Corrupting or destroying the data of other users X X X X X X X X X X X X X X X X X X X	Allowing others to access school network by sharing username and passwords		X	X						
Corrupting or destroying the data of other users X X X X X X X X X X X X X X X X X X X			X	X						
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature Continued infringements of the above, following previous warnings or sanctions Actions which could bring the school into disrepute or breach the integrity of the ethos of the school Using proxy sites or other means to subvert the school's filtering system Accidentally accessing offensive or pornographic material and failing to report the incident Deliberately accessing or trying to access offensive or pornographic material Receipt or transmission of material that infringes the copyright of another person or infringes the				X	X					
is regarded as offensive, harassment or of a bullying nature Continued infringements of the above, following previous warnings or sanctions Actions which could bring the school into disrepute or breach the integrity of the ethos of the school Using proxy sites or other means to subvert the school's filtering system Accidentally accessing offensive or pornographic material and failing to report the incident Deliberately accessing or trying to access offensive or pornographic material Receipt or transmission of material that infringes the copyright of another person or infringes the	Corrupting or destroying the data of other users		X	X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school Using proxy sites or other means to subvert the school's filtering system Accidentally accessing offensive or pornographic material and failing to report the incident Deliberately accessing or trying to access offensive or pornographic material Receipt or transmission of material that infringes the copyright of another person or infringes the	is regarded as offensive, harassment or of a		X	X	X			X		
disrepute or breach the integrity of the ethos of the school Using proxy sites or other means to subvert the school's filtering system Accidentally accessing offensive or pornographic material and failing to report the incident Deliberately accessing or trying to access offensive or pornographic material Receipt or transmission of material that infringes the copyright of another person or infringes the				X	X			X		
Accidentally accessing offensive or pornographic material and failing to report the incident Deliberately accessing or trying to access offensive or pornographic material Receipt or transmission of material that infringes the copyright of another person or infringes the				X						
pornographic material and failing to report the incident Deliberately accessing or trying to access offensive or pornographic material Receipt or transmission of material that infringes the copyright of another person or infringes the				X		X	X	X		
offensive or pornographic material Receipt or transmission of material that infringes the Copyright of another person or infringes the		X	X	X	X	X	X			
the copyright of another person or infringes the	Deliberately accessing or trying to access offensive or pornographic material			Х	X	X	X	X	X	X
	Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X	X		X	X	X	

Staff	ACII	01137	Sancti	0113				
Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X			
Inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X	X						
Unauthorised downloading or uploading of files		X						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		Х				X		
Careless use of personal data eg holding or transferring data in an insecure manner		Х				Х		
Deliberate actions to breach data protection or network security rules		Х	Х			Х		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X		X		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X	X			X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		Х	Х	Х			X	X
Actions which could compromise the staff member's professional standing		Х	Х				Х	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	Х				X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	Х	X	Х		X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	Х	Х		Х		
Deliberately accessing or trying to access offensive or pornographic material		X	Х	X	X		Х	Х
Breaching copyright or licensing regulations		Х		Х		Х		X
Continued infringements of the above, following previous warnings or sanctions		Х	Х	X	Х		X	X

Appendix 1: Reporting Log

Appendix 2: School's Acceptable Use Policy for Foundation Phase

Appendix 3: School's Acceptable Use Policy for KS2

Appendix 4: Consent forms for Photographic Images

Reporting Log

/Reporting Log School					
Date	Tme			Ináde Repor	Inádent Reported by
Inciden†					
Whataction was taken?	n?				
Who took theaction?					



Saint David's CiW Primary School

'Acceptable Use' Policy for Key Stage 2 Children

I understand that while I am a member of St David's Primary School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the School:

- I will not try to access anything illegal
- I will not download anything that I do not have the right to use.
- If I bring a mobile phone to school it will be stored away for the school day.
- I will not deliberately bypass any systems designed to keep the school safer.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the school, without permission.

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name	
Signature	
Date	



Saint David's CiW Primary School

'Acceptable Use' Policy for Foundation Phase Children'

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer
- I will only use activities that an adult has told or allowed me to use.
- I will take care of the computer and other equipment
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computer.

Childs N	Jame:	 	 	 	 	
Signed	(parent)		 	 	 	



Saint David's CiW Primary School

Use of Digital / Video Images

The use of digital / video images plays an important part in our activities. Children / young people, staff and volunteers may use digital cameras or other devices to record evidence of those activities. These images may then be used in displays and presentations and may also be used to celebrate success through their publication in newsletters, on the website, social media networks and occasionally in the public media.

The school will comply with GDPR and request parent / carer permission before taking images of their children. We will also ensure that, wherever possible, full names will not be published alongside images.

It's a great thing to film your child at our events and we know they provide a lot of precious memories. You can support us in keeping our children safe by considering the following:

- Images and video should be for your own or family's personal use only
- Think about privacy and who has the right to see your images, not only of your own child but of others
- If you do share the images online, then you must make sure they are limited to immediate family only and not public
- If you need help in knowing how to do this then come and have a chat with us

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form	
Parent / Carers Name	
Name of Child / Young Person	

PLEASE TICK BELOW

Date	
Signed	
I agree that if I take digital or video images at school events which include images of children, other than my own, I will abide by these guidelines in my use of the images.	
I agree to photos of my child being used on the school website	
As the parent / carer of the above child, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support legitimate activities or in publicity that reasonably celebrates success and promotes the work of the school.	