Saint Nicholas Owen
Catholic Multi-Academy Company

Our Lady of Fatima Catholic Primary School

E-Safety Policy

(Previously called: Safe and effective use of the Internet)

Introduction

Mission Statement

We welcome everyone into our community to live, love and learn together in the light and example of Jesus Christ.

Background

Our Lady of Fatima Primary School believes that the Internet is an essential element in 21st century life for education, business and social interaction.

The purpose of Internet use in school is:

- To raise educational standards and promote pupil achievement.
- To support the professional work of staff.
- To enhance the school's management, information and administration systems.

At Our Lady of Fatima we believe that we have a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. We also acknowledge our responsibility to ensure that pupils use the Internet appropriately and safely.

The aim of these policies is to show how pupils, teachers, parents, Academy Representatives and the wider community can use this valuable resource and means of communication to enhance the learning experiences and life skills.

Educational benefits of the Internet

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries.
- Inclusion in government and local initiatives.
- Educational and cultural exchanges between pupils world-wide.
- Cultural, social, vocational and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support including remote management of networks.
- Exchange of curriculum and administration data with the local authority and Department for Education.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming 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 or addictive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school.
We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children about the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.
Our Lady of Fatima Catholic Primary School's e-safeguarding policy has been written from a template provided by the South West Grid for Learning.

Development

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

- *C van Vliet (Head teacher)*
- *D O'Connor (E-Safety Officer / Deputy Headteacher)*
- *T Workman (Teaching Staff/ Previous ICT coordinator)*
- *K Keegan (Academy Representative)*

Consultation with the whole school 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 *Academy Representatives on:*	*Insert date* 13/05/2015
The implementation of this e-safety policy will be monitored by the:	*Headteacher* *E-Safety Coordinator/ DHT* *Academy Representative responsible for E Safety*
Monitoring will take place at regular intervals:	*Every 12 months*
The *Academy Committee* 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:	*Every 12 months*
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:	*01 May 2016*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Headteacher (DSL)* *E Safety Officer* *Local Authority Safeguarding Officer* *Police*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
  - *students / pupils*
  - parents / carers
  - *staff*

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. 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 anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

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

Academy Representatives:

Academy Representatives 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 *Academy Representatives* receiving regular information about e-safety incidents and monitoring reports. A member of the *Academy Representatives* has taken on the role of *E-Safety Academy Representative*. The role of the E-Safety *Academy Representative* will include:

- *regular meetings with the E-Safety Co-ordinator*
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to the Academy Representatives*

Headteacher and Senior Leaders:

- **The *Headteacher* has a duty of care 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 Headteacher and Deputy Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.**
- *The Headteacher and Deputy Headteacher are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.*
- *The Headteacher and Deputy 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 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 Co-ordinator.*

E-Safety Coordinator:

- leads the e-safety committee

- Responsible for ensuring that the use of the *network / internet / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be investigated / actioned / sanctioned.

  - takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
  - 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 Local Authority / relevant body
  - liaises with school technical staff
  - creates reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

- To investigate, action and sanction incidents.
  - meets regularly with E-Safety *Academy Representative* to discuss current issues, review incident logs and filtering / change control logs
  - attends relevant meeting / *Academy Representatives* committee meeting
  - reports regularly to Senior Leadership Team

ICT Coordinator:

The *Co-ordinator for ICT / Computing* is responsible for ensuring:

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the *school* meets required e-safety technical requirements and any *Local Authority* E-Safety Policy / Guidance.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- *the filtering policy provided by Link2ICT, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- *that monitoring software (Policy Central) is implemented and updated when required*

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 Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the *Headteacher / E-Safety Coordinator* for investigation / action / sanction**
- **all digital communications with students / parents / carers 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 activities

- students understand and follow the e-safety and acceptable use policies
- students 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 students 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*

For searching the Internet, in accordance with the new Computing Curriculum we do allow safe searching in the juniors with a suitable set of key words. Children are expected to use Safe Search Kids **http://www.safesearchkids.com/ (which is powered by Google with safe search enabled).**

Designated Safeguarding Lead Person

should be trained in e-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
- cyber-bullying

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. This committee is part of the safeguarding group. The group will also be responsible for regular reporting to the *Academy Representatives*.

Members of the *E-safety Group* (or other relevant group) will assist the *E-Safety Coordinator (or other relevant person, as above)* with:

- the production / review / monitoring of the school e-safety policy / documents.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

An E-Safety Group Terms of Reference Template can be found in the appendices

Pupils:

- **are responsible for using the *school* digital technology systems in accordance with the Student Acceptable Use Policy**
- 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 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. The *school* will take every opportunity to help parents understand these issues through *Parents' Evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / 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.

Community Users

Community Users who access school systems / website / VLE as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

Other policies relating to E-safety

PSHE	E-Safety has links to staying safe
Safeguarding	Safeguarding children electronically is an important aspect of E-Safety. ***This e-safety policy forms a part of the school's safeguarding policy***
Behaviour	Positive strategies for encouraging e-safety and sanctions for disregarding it.
ICT Policy	How ICT is used, managed, resourced and supported in our school.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* to take a responsible approach. The education of *students* 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 alongside the Switched on Computing scheme 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 pastoral activities**
- **Students should be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- *Students should be helped to understand the need for the student 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 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 students 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or Link2ICT) 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.*

Education – parents / carers

Parents may have 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*
- *Parents' INSPIRE workshops*
- *High profile events / campaigns eg Safer Internet Day*
- *Reference to the relevant web sites / publications e.g* www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

Education – The Wider Community

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

- *Providing family learning courses in use of new digital technologies, digital literacy and e-safety*
- *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*
- *Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision (possibly supporting the group in the use of Online Compass, an online safety self review tool - www.onlinecompass.org.uk)*

Education & Training – Staff / Volunteers

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:

- **An annual 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 regularly.** *It is expected that some staff will identify e-safety as a training need within the performance management process.*
- *The E-Safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.*
- *The E-Safety Coordinator will provide advice / guidance / training to individuals as required.*

Training – Academy Representatives

Academy Representatives should take part in e-safety training / awareness sessions, with particular importance for those who are responsible for e-safety, health and safety and child protection. This may be offered in a number of ways:

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

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users** at KS2 and above **will be provided with a username and secure password** by *the ICT Coordinator who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username and password** *and will be required to change*

their password every academic year. There will be a generic class password for KS1 and below, but the school will need to be aware of the associated risks – see appendix.

- **The " administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher* or and kept in a secure place (eg school safe)**
- The ICT Coordinator **is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**
- **Internet access is filtered for all users by Link2ICT.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes with Link2ICT.
- *The ICT Coordintor and Headteacher regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the ICT/Esafety coordinator. They will then decide what further action to take.*
- Appropriate security measures are in place by Link2ICT to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.
- A username is available for 'guests' (eg trainee teachers, supply teachers, visitors) onto the school systems. This profile is restricted.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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 students 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 eg on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students* in the digital / video images.
- *Staff and volunteers 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.*
- *Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Students must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.*

- *Students' 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 students are published on the school website*

Data Protection

All data held on the school's network is subject to the *Data Protection Act 1998* and the school's *Child Protection Policy*.

Unlicensed or personal software must not be installed on the school's hardware or connected in any way to the school's equipment or systems. If software is deemed to be of use to the school then it should be duly acquired by the school under licence.

Where data of a personal nature such as: school reports, IEPs, correspondence and assessment data is taken home on a school laptop or other portable storage media, it must be recognised that this data comes under the *Data Protection Act* and is subject to the school's *Child Protection Policy*. Care must therefore be taken to ensure its integrity and security. It should be removed from any portable device including USB pens and memory cards as soon as possible.

Where authorisation has been given to a specific user to use a potable storage medium (e.g. memory stick) it is his/her responsibility to ensure that it does not transmit any viruses onto the school's network. It is recommended that pupils refrain from using such media unattended.

Staff are encouraged to use the drives on the school network as a central repository for documents such as policy and planning files. Confidential pupil data may be safely stored here as access is only permissible through login by a member of school staff.

All pupil work is stored in their own personal folder on the network. Children's' files cannot be moved or deleted whilst logged onto a machine as a pupil user.

The servers containing these networked drives are locked away each night as an extra security measure to prevent against theft.

Data Backups

Data stored on the school's networked drives are backed up regularly so that copies of files may be recovered if the original becomes either lost or damaged.

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 & other adults			Students / Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		x					x	
Use of mobile phones in lessons								x
Use of mobile phones in social time	x							x
Taking photos on mobile phones / cameras								x
Use of other mobile devices eg tablets, gaming devices								x
Use of personal email addresses in school, or on school network		x						x
Use of school email for personal emails		x						x
Use of messaging apps								x
Use of social media							x	
Use of blogs	x						x	

When using communication technologies the school considers the following as good practice:

- **Users must immediately report, to the nominated person – in accordance with the school 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 and students or parents / carers (email, chat, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

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 usage as follows:

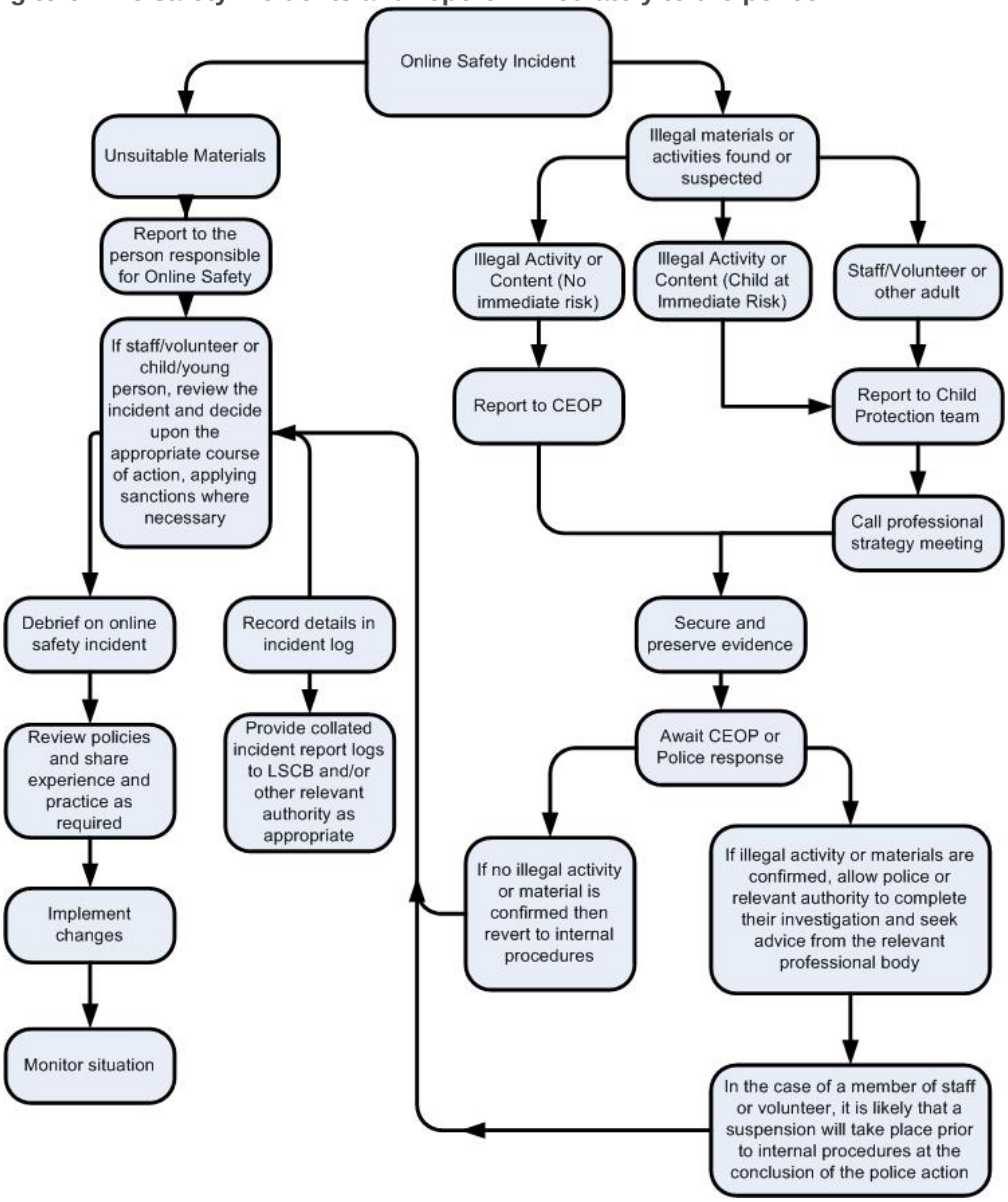
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	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					X
	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 business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)			X			
On-line gambling					X	
On-line shopping / commerce			X			
File sharing				X		
Use of social media				x		
Use of messaging apps					x	
Use of video broadcasting eg Youtube			x			

Responding to incidents of misuse

This guidance is intended for use when staff need 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 (see “User Actions” above).

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, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school 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.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- 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 in accordance with the behaviour policy.
    - Involvement by Local Authority or national / local organisation (as relevant).
    - 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 *school* 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.

School Actions & Sanctions

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 the school behaviour policy and the procedures as follows:

Pupils

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	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 detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	x							x	
Unauthorised use of mobile phone / digital camera / other mobile device	x	X	x			x			
Unauthorised use of social media / messaging apps / personal email	x	X	x		x	x		x	
Unauthorised downloading or uploading of files	x	X	x					x	
Allowing others to access school / network by sharing username and passwords	x	x						x	
Attempting to access or accessing the school / academy network, using another student's / pupil's account	x	x						X	
Attempting to access or accessing the school / academy network, using the account of a member of staff	x	x	x			X	X	x	
Corrupting or destroying the data of other users	x	x	x		x	X	X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x		x		x	x	x	X	
Continued infringements of the above, following previous warnings or sanctions			x			x			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X						x
Using proxy sites or other means to subvert the school's / academy's filtering system	x	x	x		x	x	x		
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x			x	X		x	
Deliberately accessing or trying to access offensive or pornographic material	x	x	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	x	x	

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	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				
Inappropriate personal use of the internet / social media / personal email		x			X	x		
Unauthorised downloading or uploading of files	X					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	x					X		
Careless use of personal data eg holding or transferring data in an insecure manner		x				X		
Deliberate actions to breach data protection or network security rules		x	x		x			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X						x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x		x				X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X		X				x
Actions which could compromise the staff member's professional standing		x				x		
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		x						X
Using proxy sites or other means to subvert the school's / academy's filtering system		x						X
Accidentally accessing offensive or pornographic material and failing to report the incident					X	x		
Deliberately accessing or trying to access offensive or pornographic material		x		x				X
Breaching copyright or licensing regulations					x	X		
Continued infringements of the above, following previous warnings or sanctions		x						x

Responsible Internet Use

Dear Parent/Guardian,

As part of our curriculum we encourage pupils to make use of educational resources available through supervised access to the Internet. We are also developing a Learning Platform in the form of a School Intranet which will provide a good starting point for supporting the curriculum both at school and at home and encourage independent learning.

Access to the Internet enables pupils to conduct research and obtain high quality educational resources from libraries, museums, galleries and other information sources from around the world. Access to the School Intranet provides all pupils with an online, personal storage area as well as access to online learning resources which are available anytime, anywhere.

To guard against accidental access to materials which are inappropriate in school, Our Lady of Fatima School accesses the Internet and the School Intranet by means of the Birmingham Grid for Learning (BGfL) which provides an appropriately filtered service. However, it is not possible to provide a 100% assurance that pupils might not accidentally come across material which would be inappropriate.

Therefore, we would like all pupils to discuss the attached Rules for Responsible Internet Use with their parents/guardians and then return the attached form to the school.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

We believe that the educational benefits to pupils from access to the Internet and the School Intranet, in the form of information resources and opportunities for collaboration, far outweigh the potential disadvantages.

Should you wish to discuss any concerns about Internet use in school, please telephone the school office to arrange an appointment.

Yours sincerely

Our Lady of Fatima Primary School
Responsible Internet Use

Pupil's Section

We use the school computers and Internet connection for learning.
These rules are to help us use the Internet responsibly, be fair to others and keep everyone safe.

- I will only access the Internet when my teacher gives me permission.
- I will only access websites that my teacher has approved.
- I will only use my own log on name and password and will not share my user name or password.
- I will not look at or delete other people's files.
- I will not use Internet chat.

- I will only email people that my teacher has approved.
- The messages I send will be friendly and polite.
- I will only give my email address to my friends and my family.
- I will never enter my email address into a web page on the Internet.
- I will ask permission before opening an email or attachment.
- I will never give my home address, telephone number or arrange to meet someone in an email.

- **If I see anything I am unhappy with or receive messages I do not like I will tell a teacher immediately.**
- **I understand that the school may check my computer files and monitor the Internet sites I visit.**

I have read and understand the school Rules for Responsible Internet Use. I will use the School Computers and the Internet in a responsible way.
I understand that if I break any of the terms of this contract, I could be stopped from using the Internet or computers.

Pupil's Signature …….. Class …… Date ……

……

Parental Consent for Internet Access

I have read and understand the school Rules for Responsible Internet Use and give permission for my son/ daughter to access the Internet. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials and pupils will be taught about the effective use of the Internet and online safety.

Parent's signature _____ Date _____

Parental Consent for Web Publication of Work and Photographs

I the parent of _____ agree / do not agree that if selected, my son/ daughter's work may be published on the **School Website** which is available to people outside our school community.
I also agree that photographs and other digital media that include my son / daughter may be published subject to the school rules that photographs will not clearly identify individuals and that names will not be used.

Signed ..... Date .....

Parental Consent for Publication of Work and Photographs on our School Intranet Site

I the parent of _____ agree / do not agree that if selected, my son/ daughter's work may be published on the **School Intranet Site** which I understand is password protected and only made available to members of our school community.
I also agree that photographs and other digital media that include my son / daughter may be published only after my written permission. I understand that I will be consulted on each occasion my child's photograph is used.

Signed ..... Date .....

Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

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

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……

(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent / carer should be sufficient)

Signed (parent): ……..

Parent Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They 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 communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name | Student / Pupil Name

As the parent / carer of the above *students / pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)
I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
Or: (KS1)
I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed | Date

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the Data Protection Act and request parents permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents comment on any activities involving other *students* in the digital / video images.

Parents are requested to sign the permission form below to allow the school to take and use images of their children and for the parents to agree

Digital / Video Images Permission Form

Parent Name	
Student Name	

As the parent of the above *student* , 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 learning activities or in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed	
Date	

Pupil Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the Student Acceptable Use Agreement.

It is suggested that when the Student / Pupil AUP is written that a copy should be attached to the Parents / Carers AUP Agreement to provide information for parents and carers about the rules and behaviours that students / pupils have committed to by signing the form.

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school / academy* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students and parents using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school / academy*:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / Academy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

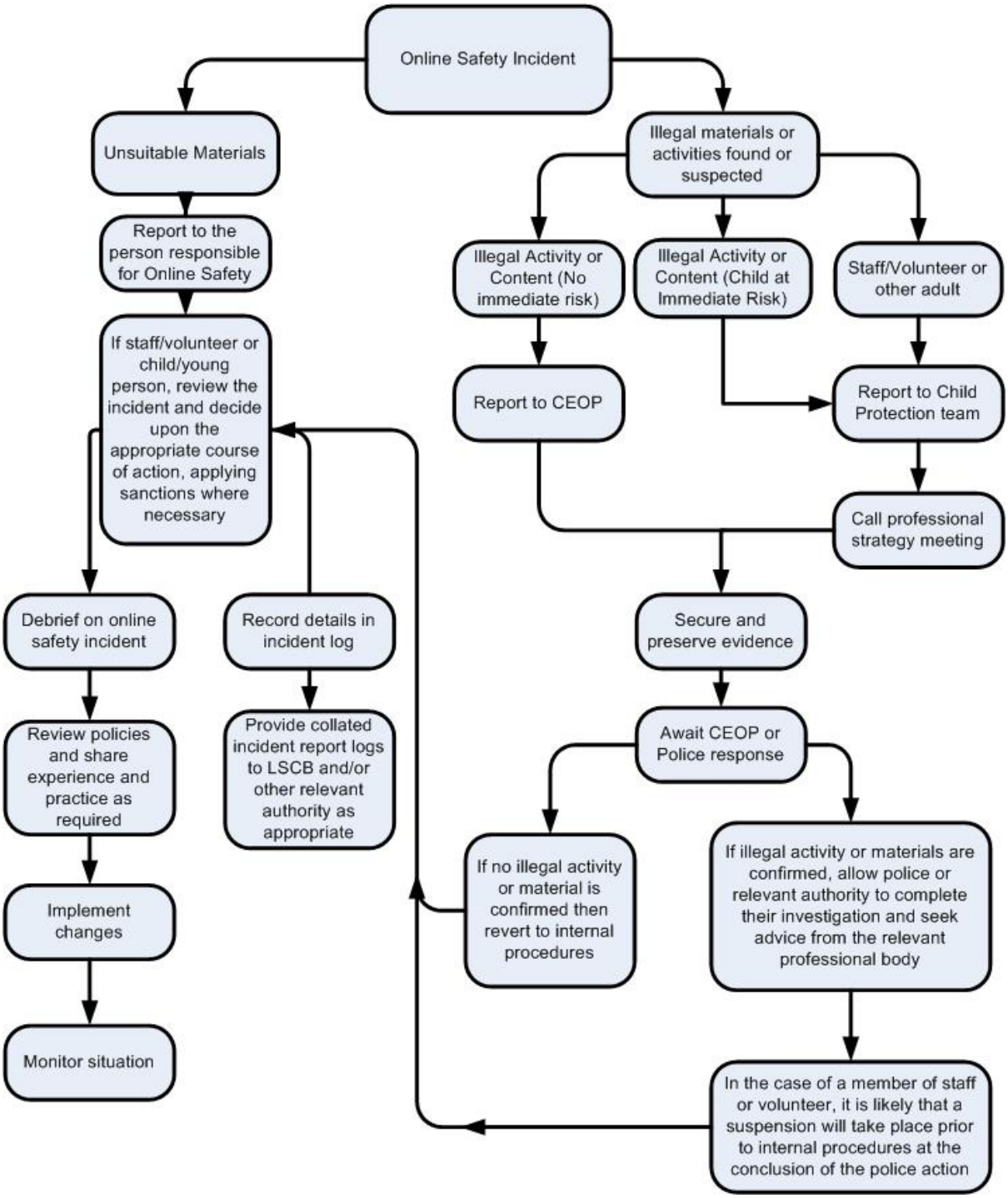
I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Responding to incidents of misuse – flow chart



Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Template Reporting Log

Reporting Log Group	Date	Time	Incident	Action taken		Incident Reported by	Signature
				What?	By whom?		

Training Needs Audit

Training Needs Audit Log
Group ..... Date .....

Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date			

School Policy - E-Safety Committee Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The e-safety committee will seek to include representation from all stakeholders.
The composition of the group should include:

- Headtecher (Child Protection/Safeguarding officer)
- Deputy Headteacher (Child Protection/Safeguarding officer)
- Support staff member
- E-safety coordinator (not ICT coordinator by default)
- Academy Representative
- *Pupil representation* – for advice and feedback. *Pupil voice is essential in the make-up of the e-safety committee, but students would only be expected to take part in committee meetings where deemed relevant.*

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. CHAIRPERSON

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. DURATION OF MEETINGS

Meetings shall be held termly for a period of 1 hour. A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the E-safety Co-ordinator (or other relevant person) with the following:

- To keep up to date with new developments in the area of e-safety
- To review and develop the e-safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the e-safety policy
- To monitor the log of reported e-safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-safety. This could be carried out through:
- Staff meetings
- Student forums (for advice and feedback)
- Academy Committee meetings

- Surveys/questionnaires for students / pupils, parents / carers and staff
- Parents evenings
- Website/VLE/Newsletters
- E-safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the [school]
- To monitor incidents involving cyberbullying for staff and pupils

6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for Our Lady of Fatima Primary School have been agreed

Signed by (E Safety Coordinator):

Date: May 2015

Reviewed: May 2016

Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safety policy.

UK Safer Internet Centre

Safer Internet Centre -

South West Grid for Learning

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP

http://ceop.police.uk/ ThinkUKnow

Others:

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm

UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis

Netsmartz http://www.netsmartz.org/index.aspx

Support for Schools

Specialist help and support SWGfL BOOST

Cyberbullying

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government Better relationships, better learning, better behaviour

DCSF - Cyberbullying guidance

DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

Digizen – Social Networking

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Alberta, Canada - digital citizenship policy development guide.pdf

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Somerset - e-Sense materials for schools

Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO

ICO pages for young people

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)

ICO - Guidance we gave to schools - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO – Access Aware Toolkit

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL - Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People

Kent - Safer Practice with Technology

Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs

Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs

UK Safer Internet Centre Professionals Online Safety Helpline

Working with parents and carers

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

SWGfL BOOST Presentations - parents presentation

Connect Safely - a Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

DirectGov - Internet Safety for parents

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

The Cybersmile Foundation (cyberbullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol