Witchampton CofE First School

E-Safety and ICT Acceptable Use Policy

As a Church of England School we are guided by our Christian values in supporting the learning of all our children.

'Live a Life of Love Just as Jesus Loved Us' Ephesians 5:2

School E-Safety Policy

Background / Rationale:

New technologies have become integral to the lives of children in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and Academy Committee members to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face by using digital devices, being online and through social media include:

- Access to illegal, harmful or inappropriate images or other content.
- Putting themselves at risk through the sharing of images such as sexting.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming/child sexploitation 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.
- Exposure to radicalisation and extremism.
- 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.

Witchampton CofE First School is committed to safeguarding its pupils. 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, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore vital, through good educational provision to build 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.

At Witchampton C of E First School we must demonstrate that we have 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 in order 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.

Development / Monitoring / Review of this Policy:

This e-safety policy has been developed by SWGfL, amended by Witchampton C of E First School and adopted by the Academy Committee.

Schedule for Development / Monitoring / Review:

This e-safety policy was approved by the academy committee members Committee on:	May 2020
The implementation of this e-safety policy will be monitored by the:	Headteacher and Academy Committee
Monitoring will take place at regular intervals:	Ongoing each Term
The Trustees of Wimborne Academy Trust will receive information on the implementation of this e-safety policy, (which will include anonymous details of e-safety incidents). At regular intervals and/or at request:	On request
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:	Annually Summer Term
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	Strategic ICT Manager, Dorset LA Louise Dodds, Safeguarding Officer

The school will monitor the impact of the policy using:

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

Scope of the Policy:

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, governors, 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 Head Teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of 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 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 roles and responsibilities for e-safety of individuals and groups within the school:

Academy Committee Members:

Academy Committee members 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 Committee receiving regular information about e-safety incidents and monitoring reports. Part of the role of the Safeguarding Academy Committee Member will be to:

- meet with the E-Safety Champion
- monitor e-safety incident logs
- monitor filtering / change control logs
- report to relevant Committee members at an Academy Committee meeting

Headteacher and Designated Safeguard Lead (DSL):

- The Headteacher (who is the DSL) 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 Champion.
- The Headteacher is responsible for ensuring that the E-Safety Champion 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 Headteacher and the Deputy DSLs 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. (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures).

E-Safety Champion:

- 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 technical support staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Academy Committee member to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings of Academy Committee members as required
- reports regularly to the Headteacher.

The E-Safety Lead 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 / other relevant body E-Safety Policy / Guidance that may apply.
- 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 (if it has one), 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

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 Champion for investigation / action / sanction

• all digital communications with students / pupils / 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 / pupils understand and follow the e-safety and acceptable use policies

• 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 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 / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead:

should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- social media
- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- sexting
- radicalisation
- child sexual exploitation

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.
- Are educated on safe usage of social media / cyberbullying/ sexting/ grooming/ CSE/ radicalisation /digital social etiquette.
- 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 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 and the use of images.
- 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' 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:

- Their child's use of digital technology outside of school.
- Digital and video images taken at school events
- Endorsing (by signature) the Pupil Acceptable Use Policy.
- Accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Policy Statements

Education – pupils:

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in 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
- Students / 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.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be helped to understand the need for the student / 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, following at all times the staff code of conduct for safer working practices
- 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.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – parents / carers:

Some parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site information
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk , www.saferinternet.org.uk, http://www.childnet.com/parents-and-carers

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:

• 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.

• 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 Agreements.

Training – Academy Committee:

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are responsible for overseeing ICT / e-safety / health and safety / child protection.

This may be offered in a number of ways:

- Attendance at training provided by the Trust / Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions 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 the e-safety technical requirements.
- There will be regular reviews and audits of the safety and security of school ICT 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 will be provided with a username and password by the Office Administrator who will keep an up to date record of users and their usernames.
- The "master / administrator" passwords for the school ICT system, used by the Office Administrator (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).

- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.
- In the event of the Office Administrator (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Any filtering issues should be reported immediately.
- Requests from staff for sites to be removed from the filtered list will be considered by the Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Office Administrator.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view user's activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Office Administrator or Headteacher
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files by users
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- Personal data such as pupil records must not be kept on laptops and should only be accessed via the secure school server.
- An agreed policy is in place that allows staff to / forbids staff from installing programmes on school workstations / portable devices.
- Memory sticks should not be used unless transferring files to a non-networked machine such as for assembly.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Instances of hacking or viruses, such as ransomware, must be reported immediately to the Head of School, Office Administrator or E-safety Champion. This includes outside of school if the remote access is likely to have been compromised.

Curriculum:

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- 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 are allowed to freely search the internet, e.g. using search engines, 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 Lexicon 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.
- 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.

Use of digital and video images - Photographic, Video:

Use of digital and video images

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

- When using digital images, staff should inform and educate students / 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
- 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 / academy events for their own personal use (as such use is 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 pupils 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

• Fairly and lawfully processed
• Processed for limited purposes
• Adequate, relevant and not excessive
• Accurate
• Kept no longer than is necessary
• Processed in accordance with the data subject's rights
• Secure
• Only transferred to others with adequate protection.

The school must ensure that:

- It has a data protection policy.
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident.
- Consideration has been given to the protection of personal data when accessed using any remote access solution.

Staff must ensure that they:

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

• Use personal data only on secure password protected computers and/or sites, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

. • Transfer data using encryption and secure password protected devices

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				Pupils			
Communication Technologies								
Mobile phones may be brought to school	X							X
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on mobile phones				X				X
Smart watches may be brought to school	X						X	
Use of smart watches in lessons				X				X
Use of smart watches in social time	X							X
Taking photos on a smart watch				X				X
Use of hand held devices e.g. e-readers, PDAs.	X							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 chat rooms / facilities		X						X
Use of instant messaging				X				X
Use of social networking sites		X						X
Use of blogs		X					X	

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, school text 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 public chat / social networking programmes must not be used for these communications).
- Whole class or group email addresses will be used in Y3- Y4 for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- 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. If deemed unacceptable, staff disciplinary procedures will follow. The school policy restricts certain internet usage as follows:

Users shall not visit Internet sites, make,	Child sexual abuse images –The making, production or distribution of indecent					x

post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	images of children. Contrary to The Protection of Children Act 1978.					
	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	
	Promotion of extremism or terrorism				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 systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy.					x	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords).					x	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet).					x	
Using school systems to run a private business					x	
Infringing copyright					x	
On-line gaming (educational)		x				
On-line gaming without means of digital communication (non-educational) * For pupils under close adult supervision as part of a reward i.e Golden Time.			x			

On-line gambling				x	
On-line shopping/commerce * Only by authorised staff in the process of procurement of goods and services.	x*				
File sharing *Using the school's chosen secure sharing facility.	x*				
Use of social media				x	
Use of messaging apps *Outside of teaching times and in the staffroom only.		x			
Use of video broadcasting e.g. Youtube *For educational use only, for pupils under close adult supervision.		x*			

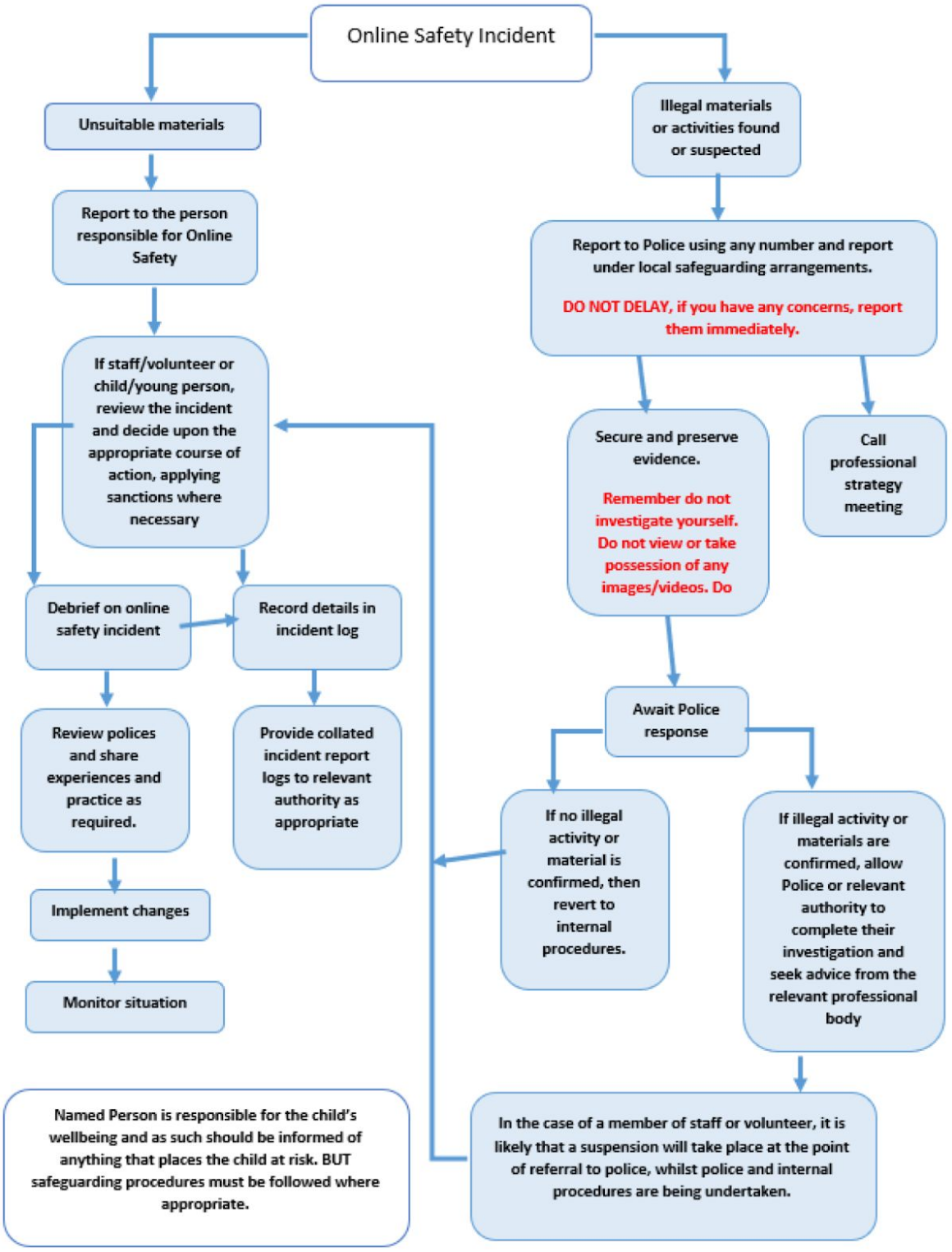
Responding to incidents of misuse:

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). Online Safety BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (https://boost.swgfl.org.uk/)

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.

The SWGfL flow chart – below and http://swgfl.org.uk/FAQs should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.


Online Safety Incident
Unsuitable materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

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
    - Involvement by Local Authority/Academy Group 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
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - 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 possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

This policy has been reviewed in line with the 9 principles set out in the Single Equality Policy and an initial screening Equality Impact Assessment has been carried out.

Signed: …… Chair of Academy Committee

Date on which policy was adopted: May 2017

Date of Review: April 2019

Date of Review: May 2020

Date for next review: May 2021

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/
Insafe - Education Resources
Somerset - e-Sense materials for schools

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note - BYOD

Data Protection Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO
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

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 Subject Access Code of Practice
ICO – Guidance on Data Security Breach Management