Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off WSAPC site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of WSAPC , but is linked to membership of WSAPC . The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

WSAPC 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 online safety behaviour that take place out of school.

Development / Monitoring / Review of this Policy

This On-line safety policy has been developed by the Health & Safety committee made up of:

- Headteacher
- Online Safety Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within WSAPC.

Governors:

Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the resource committee, receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Health and Safety Governor which covers Online safety and safeguarding.

The role of the Health & Safety and Safeguarding Governor, in relation to On-line safety, will include:

- Attendance at Health and Safety Committee meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting

Senior Leadership Team:

- The Headteache*r has* a duty of care for ensuring the safety (including online safety) of members of WSAPC community, though the day to day responsibility for online safety will be delegated to the ICT Manager / Business Manager.
- The Headteacher / Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body* disciplinary procedures).
- The Headteacher / Senior Leadership Team are responsible for ensuring that the Online safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team / Senior Leadership Team will receive regular monitoring reports from the Online safety Co-ordinator / Business Manager

Online safety Coordinator: (ICT Development Manager /Business Manager)

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing WSAPC online safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Health & Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

ICT Development Manager / Data & Communication Manager:

The ICT Development Manager is responsible for ensuring:

- that WSAPC's technical infrastructure is secure and is not open to misuse or malicious attack
- that WSAPC meets required online safety technical requirements and any Local Authority / other relevant body Online 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

- filtering / proxy arrangements are 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 online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / sharepoint / on-line learning platforms / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported
- that monitoring software / systems are implemented and updated as agreed

Teaching and Support Staff

Teaching Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current On-line 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 / Senior Leader Team / Online safety Coordinator
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the online 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

Child Protection / Safeguarding Designated Persons / Officer

should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Health & Safety Committee

The Health and Safety Committee provides a consultative group that has wide representation from WSAPC community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

The group will also be responsible for regular reporting to the *Governing Body.*

Members of the *Health and Safety Group* will assist the *Online safety Coordinator (or other relevant person, as above)* with:

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

Students / pupils:

- are responsible for using WSAPCs digital technology systems in accordance with the Student / Pupil 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 online safety practice when using digital technologies out of school and realise that WSAPC's On-Line Safety Policy covers their actions out of school, if related to their membership of WSAPC

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. WSAPC will take every opportunity to help parents/carers understand these issues through review days, newsletters, letters home, website / online learning platforms and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support WSAPC in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parent pupil records and online learning platforms.
- their children's personal devices in WSAPC (where this is allowed)

Other Users

Other users, who access school systems as part of the wider *school* will be expected to sign an Other User Acceptable Use Policy, before being provided with access to school systems.

Policy Statements

Education – students / pupils

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

At WSAPC, On-Line Safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of ICT, PHSE and other lessons and should be regularly revisited
- Key online safety messages are reinforced as part of a planned programme of pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils will 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
- in lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (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 other relevant designated person) 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

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's 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.

WSAPC will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Website, Letters home
- Review Days

- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg ww(see appendix for further links / resources)w.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community
WSAPC will provide opportunities for local community groups / members of the community to gain from WSAPC's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- WSAPC website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision

Education & Training – Staff / Volunteers
It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand WSAPCs Online safety policy and Acceptable Use Agreements.
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from WSGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required

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

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

Technical – infrastructure / equipment, filtering and monitoring
Senior Leaders / Governors will be responsible for ensuring that WSAPC 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 online safety responsibilities:

- School technical systems will be managed in ways that ensure that WSAPC meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of schools technical systems
- Servers, wireless systems and cabling will 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 team *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 6 weeks.* WSAPC may choose to use group or class log-ons and passwords for KS1 and below
- The "master / administrator" passwords for WSAPCs ICT system, used by the Network Manager (or other person) must be available to the Senior Leadership Team or other nominated senior leader and kept in a secure place (password protected document on Sharepoint)
- ICT Development Manager 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**.** 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
- WSAPC has provided enhanced / differentiated user-level filtering
- WSAPC technical staff regularly monitor and record the activity of users on WSAPC technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system (online Health & Safety reporting) is in for users to report any actual / potential technical incident / security breach to the relevant person, as agreed
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of WSAPC systems and data. These are tested regularly. WSAPC infrastructure and individual workstations are protected by up to date virus software.
- An agreed protocol is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto WSAPC systems. (AUP Others)
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / other users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data

cannot be sent over the internet or taken off WSAPC 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 / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils 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 WSAPC 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 / 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.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at WSAPC 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 / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow WSAPC policies concerning the sharing, distribution and publication of those images. Those images should only be taken on WSAPC equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the WSAPC into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the WSAPC website
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

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 WSAPC must ensure that:

- 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.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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 other devices, 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.

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

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with WSAPC policy (below) once it has been transferred or its use is complete

Communications

The WSAPC uses its website, E-mail, telephone, mobile phones, SIMS InTouch and twitter to communicate with stakeholders and the community.

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only WSAPC email service to communicate with others when in school, or on school systems (e.g by remote access).
- Users must immediately report, to the nominated person – in accordance with WSAPC 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 / pupils or parents / carers (email, on-line learning platform etc.) must be professional in tone and content. These communications may only take place on official (monitored) school / academy systems. Personal email addresses, text messaging on personal phones or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Students / pupils should be taught about online 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 WSAPC website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

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

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

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

School staff should ensure that:

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

WSAPC's use of social media (Twitter) for professional purposes will be checked regularly by the senior risk officer and online safety committee to ensure compliance with the Social Networking Policy, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

WSPAC 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. WSAPC 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	

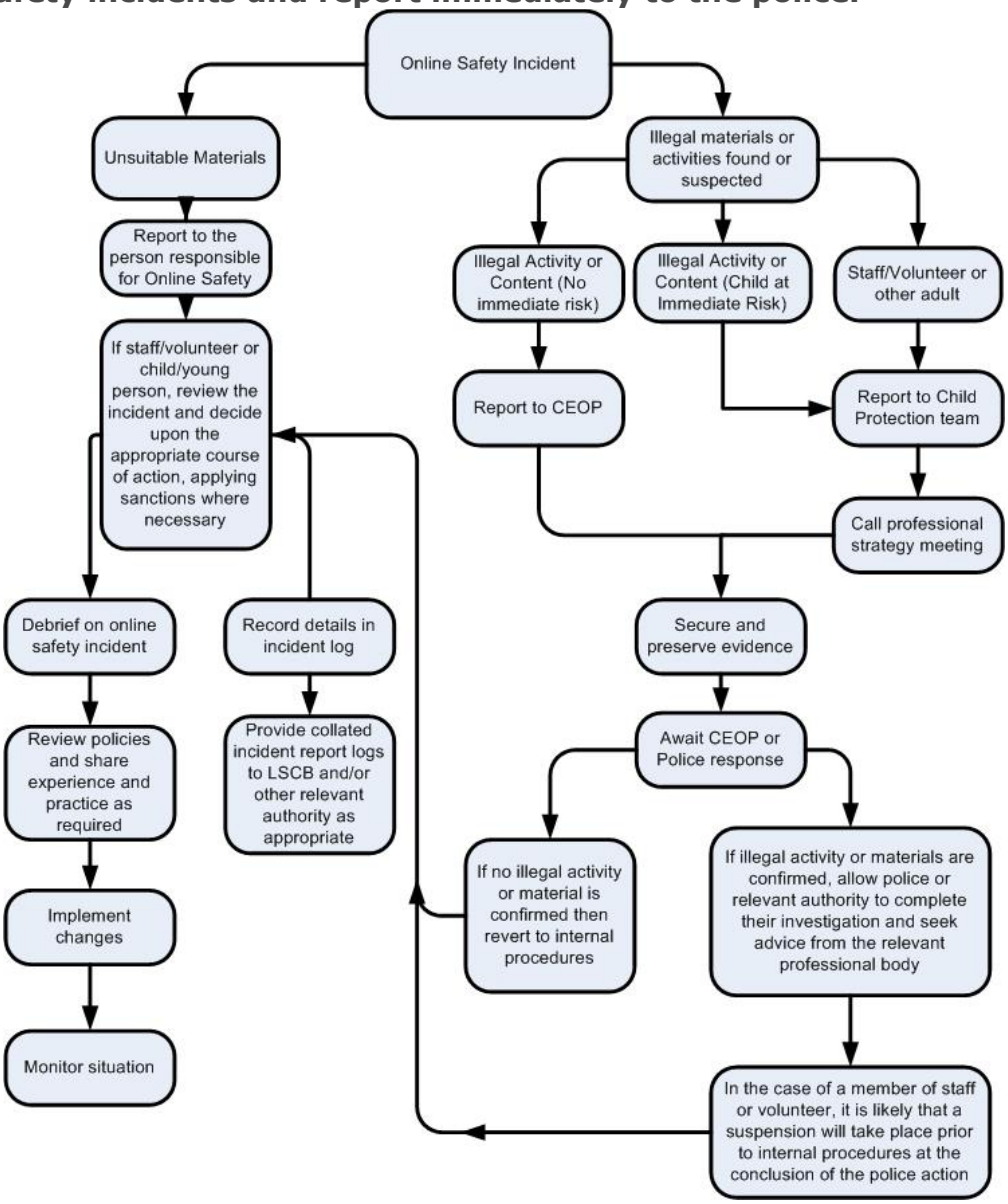
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of WSAPC or brings WSAPC into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by WSAPC / 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 WSAPC 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 with reference to other related policies and guidance which could include WSCC carrying out Investigation Guidance, Disciplinary, and Confidential Reporting. *(Linked policies are referenced at the end of this policy*):

- The investigating officer should be a senior member of staff and more than one person should be involved in the investigation 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 Investigation Officer 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 / Multi-Agency (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 WSAPC and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed investigation report(s) and evidence should be retained.

School Actions & Sanctions

It is more likely that WSAPC 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 WSAPC community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher / key worker	Refer to Assistant Headteacher	Refer to Headteacher / SLT	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 i.e. isolation / 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	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			
Unauthorised use of social media / messaging apps / personal email		x	x		x	x			
Unauthorised downloading or uploading of files			x		x	x			
Allowing others to access school network by sharing username and passwords			x		x	x			
Attempting to access or accessing WSAPC network, using another student's / pupil's account			x	x		x		x	
Attempting to access or accessing WSAPC network, using the account of a member of staff			x	x	x			x	
Corrupting or destroying the data of other users				x					
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x			x		x	x
Continued infringements of the above, following previous warnings or sanctions		x	x	x	x	x	x		x
Actions which could bring WSAPC into disrepute or breach the integrity of the ethos of WSAPC			x						
Using proxy sites or other means to subvert WSAPC'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						
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x						

Staff (inc. Agency/voluteers etc) Actions / Sanctions

	Refer to Line Manager / Assistant Headteacher	Refer to Headteacher / SLT	Refer to WSCC / Capita HR	Refer to Police	Refer to technical support staff for action re filtering / security etc	Warning	Disciplinary Action	Suspension	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x	x	x	x	x	
Inappropriate personal use of the internet / social media / personal email	x	x				x	x		
Unauthorised downloading or uploading of files		x			x	x			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing WSAPC network, using another person's account		x				x	x	x	
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x					x		
Deliberate actions to breach data protection or network security rules		x	x	x			x	x	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		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		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	x	x				x	x		
Actions which could compromise the staff member's professional standing		x	x				x		

Actions which could bring WSAPC into disrepute or breach the integrity of the ethos of WSAPC		x	x				x	x	
Using proxy sites or other means to subvert WSAPC's / academy's filtering system		x	x		x	x	x		
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x					x		
Deliberately accessing or trying to access offensive or pornographic material		x	x	x	x	x		x	
Breaching copyright or licensing regulations	x	x				x	x		
Continued infringements of the above, following previous warnings or sanctions		x	x			x	x	x	

Linked Policies

- Acceptable Use Policy Agreement (Parent/Carers / Pupils / Staff / Others)
- Behaviour at Work Policy
- CCTV/ Digital Images Policy
- Child Protection and Safeguarding policy
- Cloud Storage Policy
- Confidential Reporting Policy
- Data Protection Statement
- Disciplinary Policy
- Equality Policy
- Health & Safety Policy
- School Health & Safety Committee contacts
- School Technical Security Policy
- Social Media & Networking policy
- Staff & Pupil Privacy notice
- WSCC code of Conduct

ADOPTED BY WSAPC	January 2017
RATIFIED BY GB	January 2017
REVIEWED (annually)	January 2018
REVIEW DUE	January 2019