Scope of the Policy

This policy applies to all members of the WSAPC community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school 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 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 Online Safety Policy has been developed by the Health and Safety Committee made up of:

- Headteacher
- Staff – including Teachers, Support Staff, Technical Staff
- Online Safety Lead
- 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 and Safety and Safeguarding Governor, in relation to online 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 meetings

Senior Leadership Team

- The Headteacher 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 Network 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 all 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 will receive regular monitoring reports from the Network Manager/Business Manager.
- The Senior Leadership Team will ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

Online Safety Lead (Deputy Headteacher – Ben Thomas)

The Online Safety Lead:

- Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing WSAPC online safety policies/documents
- Provides training and advice for staff
- Liaises with the Local Authority and any other 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 and 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.

Network Manager/Data & Communication Manager

The Network Manager is responsible for ensuring that:

- WSAPC's technical infrastructure is secure and is not open to misuse or malicious attack
- WSAPC meets required online safety technical requirements and any Local Authority/other relevant body Online Safety Policy/guidance that may apply
- Users may only access the networks and devices through a properly enforced password protection policy
- The filtering policy (WSAPC excluding Chalkhill)/proxy policy (Chalkhill only) is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person. WSAPC's filtering is provided through FortiGate servers with the support of DMS, and Chalkhill's proxy servers are maintained by eSafety4Schools, in line with good practice
- 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
- The use of the network/internet/SharePoint/online learning platforms including Teams/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leadership Team/Online Safety Lead for investigation/action/sanction
- Monitoring software/systems (FortiGate and Impero) are implemented and updated as agreed in WSAPC policies.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current WSAPC Online Safety Policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP) and any other relevant policies and agreements
- They report any suspected misuse or problem to the Headteacher/Senior Leadership Team/Online Safety Lead

- All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the online safety and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

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

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Online bullying (often referred to as cyberbullying).

Health and Safety Committee

The Health and Safety Committee provides a consultative group that has wide representation from the WSAPC community, with responsibility for issues regarding online safety and the monitoring of 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 Committee* will assist the *Online Safety Lead (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/digital literacy curricular provision – ensuring relevance, breadth and progression

- Monitoring network/internet/filtering/incident logs
- Consulting stakeholders – including parents/carers and the pupils about the online safety provision
- Assist in the identification and monitoring of staff training needs in relation to all areas of online safety, including data security.

Pupils:

- Are responsible for using the WSAPC 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 online bullying
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that WSAPC's Online 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/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), including government-issued laptops.

Other Users

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

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety 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, online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides 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 online and be guided to validate the accuracy of information
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (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 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.

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

- Curriculum activities
- WSAPC website and letters home
- Review Days
- Informative briefings and Training
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g.
    - www.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 WSAPC's Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. 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 Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any subcommittee/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 (e.g. 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 school 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. WSAPC may choose to use group or class logons and passwords for KS1 and below
- The "master/administrator" passwords for WSAPC's ICT system, used by the Network Manager, Senior IT Technicians and managed service provider must be available to the Senior Leadership Team or other nominated senior leader and kept in a secure place
- The Network 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

- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- WSAPC has provided enhanced/differentiated user-level filtering, allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/guests
- 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 and Safety reporting) is in place 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, workstations, 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 (Acceptable Use Agreement/Policy for Other Users) is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto WSAPC systems.
- Agreed policies (Staff Laptop Agreement, Student Laptop Agreement and applicable Acceptable Use Policies/Agreements) are in place regarding the extent of personal use that users (staff/pupils/other users) and their family members are allowed on school devices that may be used out of school.
- Technologies are in place that forbid users from downloading executable files and installing applications on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. 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.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be WSAPC owned/provided or personally owned (in the case of visitors) and might include smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising WSAPC's wireless network. The device then has access to the wider internet which may include WSAPC's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational or for CPD/training purposes. Use of mobile technologies should be consistent with and inter-related to other relevant WSAPC polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy/agreement, and policies around theft or malicious damage.

Teaching about the safe and appropriate use of mobile technologies should be an integral part of WSAPC's online safety education programme.

- WSAPC's Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies

- WSAPC allows:

	School (WSAPC) Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	-	-	-	*No*	*Yes – filtered as "Guest/ BYOD"*	*Yes – filtered as "Guest/ BYOD"*
No network access	-	-	-	*Yes*	*Yes*	*Yes*

WSAPC owned/provided devices:

- Will be allocated to staff and pupils/students as appropriate. Staff will be allocated a desktop and/or a laptop computer, depending upon their role. Some staff may also be allocated a mobile phone. Pupils/students will have access to shared devices (desktop/laptop/tablet) or will be allocated a device (laptop) depending upon the WSAPC offering.
- Staff will be expected to bring their allocated devices with them whenever they are in centre.
- Staff will take full responsibility for the security and safety of any school-provided equipment.
- Levels of network access and internet filtering are dependent upon user (staff, pupil/student).
- Management of devices/installation of apps/changing of settings/monitoring will be performed by WSAPC Technical Staff only.
- Technical support will be provided by WSAPC Technical Staff only.
- Filtering of devices is done through in-centre FortiGate filtering (all sites excluding Chalkhill) or by proxy filtering (at Chalkhill through eSafety4Schools).
- Access to cloud services will be provided as appropriate to users.
- Data protection policies apply.

[1] Authorised device – purchased by the pupil/family through a school/LA-organised scheme or provided by the government under the DfE COVID Technology/other applicable scheme. This device may be given full access to the network as if it were owned by WSAPC.

- When staff leave WSAPC their device/s is/are returned to the Technical Staff for processing.
- WSAPC will protect devices by way of warranty. Liability for damage outside of the warranty will not fall to WSAPC. Behaviour and Acceptable Use Policies/Agreements apply.
- WSAPC will provide staff training for allocated devices.

Personal devices:

- Students are not allowed to use personal devices in school.
- Visitors may bring their own devices for the purposes of delivering training or educational sessions to staff, pupils, parents/carers, any other relevant recipient.
- Devices connected to the WSAPC wireless network will be subject to the same filtering as any other device, WSAPC-owned or not.
- Devices will not be given any other network access.
- Technical support is not provided for personal devices.
- Should WSAPC have any reason to suspect misuse of internet access, this will be dealt with under the remit of safeguarding, behaviour, disciplinary or such relevant policy.
- WSAPC will not be held liable for loss/damage or malfunction following access to the network.
- Personal devices should be readily identifiable.
- Visitors will be informed of school requirements.
- Education about the safe and responsible use of mobile devices is included in WSAPC's online safety education curriculum.

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 pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying 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. 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 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 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or WSAPC into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- 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 pupils are published on the WSAPC website or social media.
- 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.

WSAPC must ensure that:

- It has a Data Protection Policy.
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.

- It has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- It has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- It has a Data Map in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- It will hold only 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. WSAPC should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- It provides staff, parents, volunteers, teenagers and older children with information about how WSAPC looks after their data and what their rights are in a clear Privacy Notice.
- Procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- It understands how to share data lawfully and safely with other relevant data controllers.
- It reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law.

It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.

- It must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- Data must be encrypted and password protected.
- Device must be password or passcode protected.
- Device must be protected by up to date virus and malware checking software
- Data must be securely deleted from the device, in line with WSAPC policy once it has been transferred or its use is complete.

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
- Can recognise a possible breach, understand the need for urgency and know who to report it to within WSAPC
- Can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to within WSAPC
- Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- Will not transfer any WSAPC personal data to personal devices except as in line with school policy
- Access personal data sources and records 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

Communications

WSAPC uses its website, email, 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 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 pupils or parents/carers (email, Teams, online learning platform etc.) must be professional in tone and content. These communications may only take place on official (monitored) WSAPC 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 pupils at KS2 and above may be provided with individual school email addresses for educational use.
- 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 the WSAPC website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

WSAPC has 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, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render WSAPC or the 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:

- Ensuring that personal information is not published
- Training is provided including 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

WSAPC staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or WSAPC staff

- They do not engage in online discussion on personal matters relating to members of the WSAPC community
- Personal opinions should not be attributed to WSAPC or the Local Authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official WSAPC social media (Twitter) accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including:
    - Systems for reporting and dealing with abuse and misuse
    - Understanding of how incidents may be dealt with under WSAPC disciplinary procedures

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with WSAPC or impacts on WSAPC, it must be made clear that the member of staff is not communicating on behalf of WSAPC with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon WSAPC are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- WSAPC permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the internet for public postings about WSAPC
- WSAPC should effectively respond to social media comments made by others according to a defined policy or process
- WSAPC's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Lead/Health and Safety Committee to ensure compliance with WSAPC policies.

Dealing with 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	
	Promotion of extremism or terrorism				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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: - Gaining unauthorised access to school networks, data and files, through the use of computers/devices - Creating or propagating computer viruses or other harmful files - Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)						X

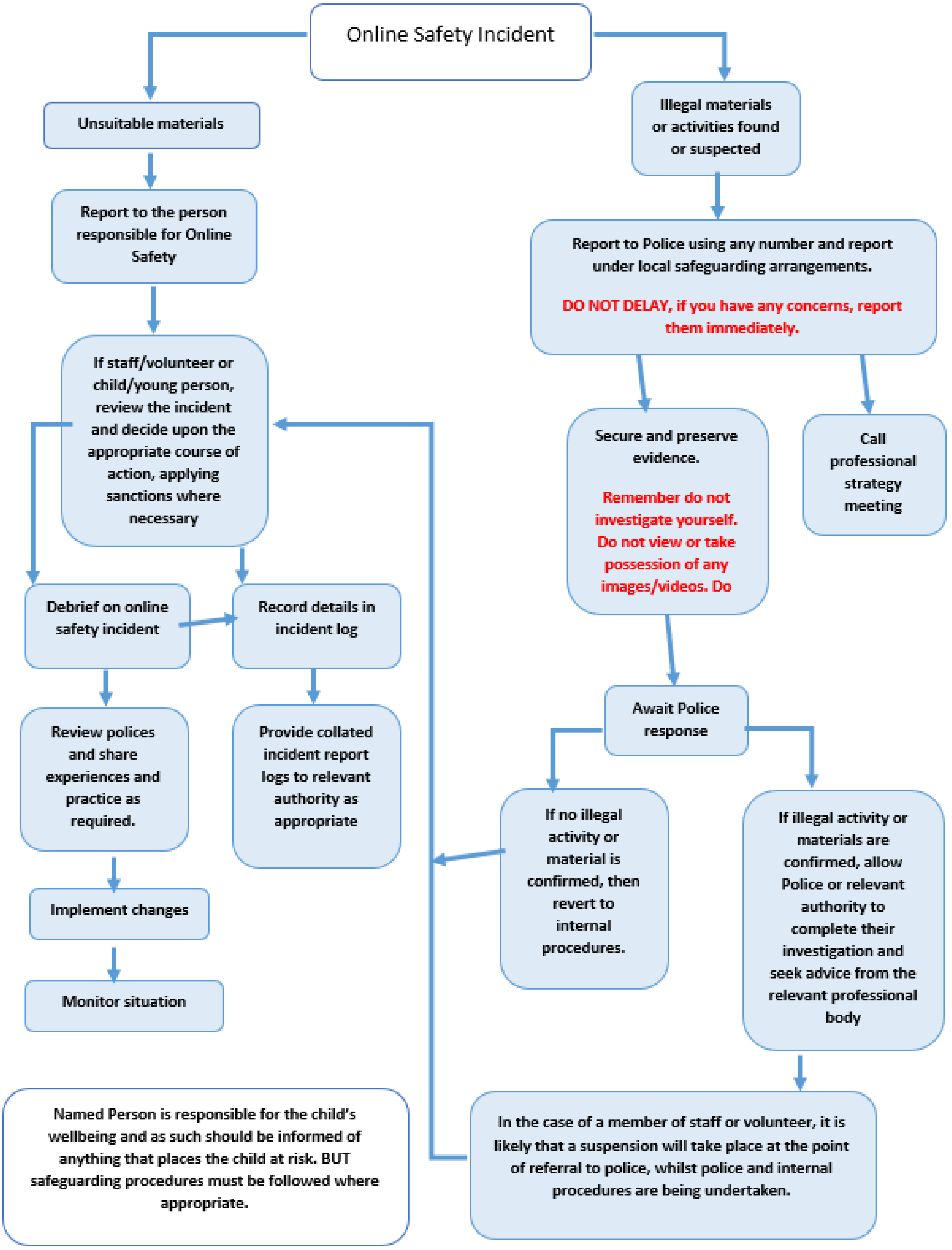
Disable/impair/disrupt network functionality through the use of computers/devices Using penetration testing equipment (without relevant permission)					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by WSAPC				X	
Revealing or publicising 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 WSAPC systems to run a private business				X	
Infringing copyright				X	
Online gaming (educational)		X			
Online gaming (non-educational)				X	
Online gambling				X	
Online shopping/commerce		X			
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. 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) for responding to online safety incidents and report immediately to the police.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

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

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

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

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 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, 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*):

- 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 or Multi-Agency Team (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.

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						

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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

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 the 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:

Staff (inc. Agency/voluteers etc)

	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 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 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)
- Student Laptop Agreement
- Staff Laptop Agreement
- Mobile Phone Policy
- Behaviour at Work Policy
- CCTV/Digital Images Policy
- Child Protection and Safeguarding policy
- Cloud Storage Policy
- Confidential Reporting Policy
- Data Protection Policy
- Disciplinary Policy

- Equality Policy
- Health and Safety Policy
- School Health and Safety Committee contacts
- Social Media & Networking policy
- Staff & Pupil Privacy notice
- Technical Security Policy
- Freedom of Information Policy
- Communications Protocol
- WSCC code of Conduct

ADOPTED BY WSAPC	January 2017
RATIFIED BY GB	January 2017
REVIEWED (annually)	August 2020
REVIEW DUE	August 2021