PARK HIGH SCHOOL

Digital Safety Policy

UPDATED	April 2019
AUTHOR	Karen Wilkinson
DOCUMENT OWNER	WSC
VERSION No	1.0
NEXT REVIEW	April 2020
REVIEWED BY	WSC

Changes, additions and comments to existing policy

This policy has been extensively revised as of April 2018. The policy has been adapted from a recommended model policy from the UK Safer Internet Centre. (https://www.saferinternet.org.uk/)

Park High School Digital Safety Policy

Digital Safety encompasses internet technologies and electronic communications such as mobile phones, tablets and wireless technology, including smart watches. Appropriate use of programmes such a Google Drive or Google classroom, learning platform, or any other file sharing and synchronization is also included. It highlights the need to educate children and young people 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 school's Digital Safety policy will operate in conjunction with other policies including those for Student Behaviour, Anti-Bullying, Curriculum, GDPR, ICT, Safeguarding and Child Protection and Vulnerable Children (with particular emphasis on the PREVENT strategy and Child Sexual Exploitation).

In addition, this policy takes into consideration the following documents or guidance

National and Local

- Harrow LSCB guidance and procedures
- Keeping Children Safe in Education (DfE, September 2018)
- Working together to safeguard children
- Sexual violence and sexual harassment between children in schools and colleges
- Protecting children from radicalisation: the prevent duty

Development, monitoring and review of this policy

This Digital Safety policy has been developed by a working group made up of:

- Headteacher and Senior Leaders (including the Designated Safeguarding Lead, Network Manager and Champion Governor)
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers

Consultation with the school has taken place through a range of formal and informal meetings.
The school will monitor the impact of the policy using:

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

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers 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 Digital Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Digital Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the Digital Safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Digital Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the WSC sub-committee receiving regular information about Digital Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Digital Safety Governor. The role of the Digital Safety Governor will include:

- regular meetings with the Digital Safety Co-ordinator
- attendance at Digital Safety Group meetings
- regular monitoring of Digital Safety incident logs
- regular monitoring of filtering
- reporting to relevant Governors

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including Digital Safety) of members of the school community, though the day to day responsibility for Digital Safety will be delegated to the Designated Safeguarding Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Digital Safety allegation being made against a member of staff. (see flow chart on dealing with Digital Safety incidents – included in a later section – "Responding to incidents of misuse".

Designated Safeguarding Lead

Should be trained in Digital Safety issues and be aware of the potential for serious child protection or 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
- leads the Digital Safety Group

- takes day to day responsibility for Digital Safety issues and has a leading role in establishing and reviewing the school Digital Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of a Digital 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 Digital Safety incidents and creates a log of incidents to inform future Digital Safety developments.
- meets regularly with Digital 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:

The Network Manager 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 Digital Safety technical requirements and any Local Authority Guidance that may apply, including liaising with LGFL.
- 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 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 Digital Safety technical information in order to effectively carry out their Digital Safety role and to inform and update others as relevant
- that the use of the network is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher or DSL for investigation.
- that monitoring software is implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of Digital Safety matters and of the current school Digital Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the DSL for investigation
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- Digital Safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Digital Safety Policy 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

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- 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 or use of images, and on cyber-bullying.
- should understand the importance of adopting good Digital Safety practice when using digital technologies out of school and realise that the school 's Digital Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and local Digital Safety campaigns and associated literature. Parents and carers will be encouraged to support the school in promoting good Digital Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the school (where this is allowed)

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 Digital Safety is therefore an essential part of the school 's Digital Safety provision. Children and young people need the help and support of the school to recognise and avoid Digital Safety risks and build their resilience.

Digital Safety should be a focus in all areas of the curriculum and staff should reinforce Digital Safety messages across the curriculum. The Digital Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Digital Safety curriculum should be provided as part of Computing /ICT/ PSCHEe / other lessons and should be regularly revisited
- Key Digital Safety messages should be reinforced as part of a planned programme of assemblies and tutorial and pastoral activities

- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupils 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 may only have a limited understanding of Digital Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings or sessions
- High profile events and campaigns e.g. Safer Internet Day
- Reference to the relevant web sites and publications

Education & Training – Staff / Volunteers

It is essential that all staff receive Digital Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Digital Safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive Digital Safety training as part of their induction programme, ensuring that they fully understand the school Digital Safety Policy and Acceptable Use Agreements.

Training – Governors

Governors should take part in Digital Safety training and awareness sessions, with particular importance for those who are members of WSC. This may be offered in a number of ways:

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

Technical – infrastructure, equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure and 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 Digital Safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager. Users are responsible for the security of their username and password and will be required to change their password every term.
- The “administrator” passwords for the school ICT system, used by the Network Manager (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)
- 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 should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- The school has provided a differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual or potential technical incident or 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 the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school.
- 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 the school site unless safely encrypted or otherwise secured**.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned, provided or personally owned and might include: smartphone, tablet, notebook, laptop or other technology that usually has the capability of utilising the school 's wireless network. The device then has access to the wider internet which may include the school '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 or personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school 's Digital Safety education programme.

- The school Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies
- The school allows:

	School 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[2]	Yes	Yes
Full network access	Yes	Yes	Yes	No[3]	No	No
Internet only	No	No	No	No	No	Yes[4]

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 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 possible for future employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

[1] Authorised device – purchased by the pupil/family through a school -organised scheme. This device may be given full access to the network as if it were owned by the school.

[2] With the exception of pupils in Year 12/13, and (on occasion and only via prior agreement) some school trips.

[3] With the exception of pupils in Year 12/13

[4] Only available via a visitor pass distributed by IT support

- 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.

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 events for their own personal use (as such use in not covered by GDPR). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital or video images.
- Staff and volunteers are allowed to take digital or 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 or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupils and parents or carers.

GDPR

Personal data will be recorded, processed, transferred and made available according to the GDPR legislation 2018 which states that personal data must be:

- processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected

The school 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 GDPR policy
- It is registered as a Data Controller for the purposes of GDPR
- Responsible persons are appointed- 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 and cloud computing which ensure that such data transfer and 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 school policy (below) once it has been transferred or its use is complete

Communications

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. Users should be aware that email communications are 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 must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about Digital Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

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 the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- 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

School staff should ensure that:

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

When official school social media 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 school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school 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
- The school 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 the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

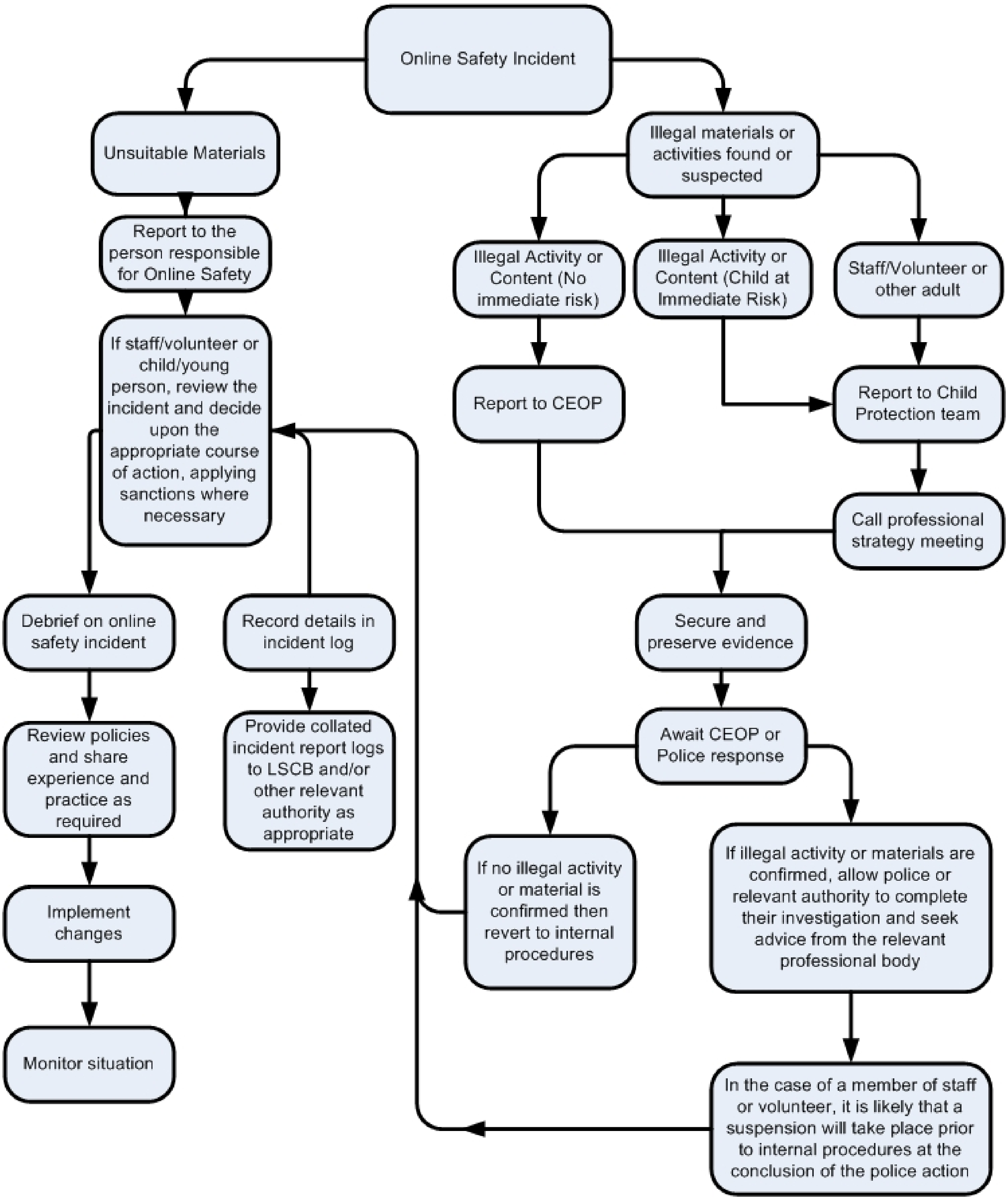
The school 's use of social media for professional purposes will be checked regularly by the School Marketing & Communications Officer and DSL to ensure compliance with the school policies.

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.

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 Digital 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
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or 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
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

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 / volunteer 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 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
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour and disciplinary procedures.

Further information and links to advice and guidance for parents may be found on the school website.

Appendix A: Abbreviations used

AHT – Assistant Headteacher
CAF – Common assessment framework
CP – Child protection
CSE – child sexual exploitation
DFE- Department for Education
EAL – English as an additional language
FGM – female genital mutilation
FSM – Free school meals
GDPR- General Data Protection Regulations
ICT- Information Communications Technology
LA-Local Authority
LSCB – local safeguarding children board
PSCHEe- Personal, Social, Citizenship, Economic Education
PSA – pastoral support assistant
SEMH- Social, Emotional and Mental Health
SENDCO- Special educational needs and Disability Co-Ordinator
SEN/D – Special educational needs and Disability
SLT – Senior Leadership Team
WSC- Whole School and Community