



Kingsway PRIMARY SCHOOL

School Online Safety Policy			
CURRENT POLICY REDRAFT/AMENDMENTS	No	<i>If Yes please provide brief details of changes below and highlight changes in yellow.</i>	
NEW POLICY	Yes	AUTHOR	Germaine Mckinnon
LAST REVIEWED	March 2026	NEXT REVIEW	March 2027
REVIEW CYCLE	Annually	TO BE RATIFIED BY TRUSTEES	No
		TO BE RATIFIED BY THE LGB	Yes
DATE APPROVED BY LGB			
Name of LiFE MAT School:	Kingsway Primary School		

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 the academy community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of academy digital technology systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. 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. This policy has been written following KCSIE 2023.

The academy 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.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the academy:

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 Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Coordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors Committee

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety 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 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 relevant body disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead 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 and Senior Leaders 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 those colleagues who take on important monitoring roles. For example, there will be at least two people who carry out such monitoring.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/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/MAT/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 Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team

Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required online safety technical requirements and any Local Authority/MAT/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
- 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 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 networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders; Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- All staff must have read KCSIE2023 - online safety section is point 135 - 151

- they have an up to date awareness of online safety matters and of the current academy online safety policy and practices
- they have read, understood and signed the staff acceptable use policy (AUP) • they report any suspected misuse or problem to the Headteacher/Senior Leader/Online Safety Lead for investigation/action/sanction
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems - Class Dojo
- online safety issues are embedded in all aspects of the curriculum and other activities • pupils understand and follow the Online 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 students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead/Designated Person/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
- online-bullying

Pupils:

- are responsible for using the academy 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/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 the academy's online 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 academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the academy 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 parents' sections of the website/Learning Platform and on-line pupil

records

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/digital literacy is therefore an essential part of the academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should 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 should be provided as part of Computing/PHSE/other lessons and should be regularly revisited

- Key online safety messages should be reinforced as part of a planned programme of assemblies and 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.
- 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 pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside academy. • 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 possible, children should use child friendly search engines, such as swiggle, which limits the results that children have access to, to only those that are safe and friendly. • 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.

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

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Social media updates on a regular basis with current guidance and resources • Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, <http://www.childnet.com/parents-and-carers> (see *appendix for further links/resources*)

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.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school/academy online safety policy and acceptable use agreements. • It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL/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/training sessions.
- 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 group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/MAT/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in academy training/information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring The school/academy will be responsible for ensuring that the academy infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. This section relates to KCSIE 23 141-148 and should be read in conjunction with the Department of Education standards for filtering and monitoring standards.

<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges>

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:

- academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of academy technical systems •

Servers, wireless systems and cabling must be securely located and physical access restricted • All users will have clearly defined access rights to academy technical systems and devices. • All users (at KS2 and above) will be provided with a username and secure password by Mr P

Johnson/Mr N Devine who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.

- The “master/administrator” passwords for the academy systems, 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 (academy safe)
- Mrs T Brooks in conjunction with N Devine/P Johnson 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.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The academy has provided enhanced/differentiated user-level filtering
 - academy 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/potential technical incident/security breach to the relevant person.
- 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 devices 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. We have a generic ‘Supply’ account for supply teachers and trainee teachers will be provided with a temporary account which is disabled when their placement finishes.
- An agreed policy is in place regarding the extent of personal use that users (staff/pupils/community 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 (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 cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and interrelated to other relevant school policies 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 online safety education programme.

- The school acceptable use agreements for staff, pupils/students 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 ²
Full network access	Yes	Yes	Yes	No No	No

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 The school should add below any specific requirements about the use of mobile/personal devices in school

Internet only				No No	No
No network access				Yes Yes	Yes

Aspects that the school may wish to consider and be included in their online safety policy, mobile technologies policy or acceptable use agreements:

Personal devices:

If staff bring a device into school it is at their own personal risk.

They must not use a device in front of pupils unless there is an emergency situation.

Pupils will not be able to bring in their own devices.

Staff may use their own devices for school business but they will not be allowed access to the school systems.

There will be no technical support available for devices brought from home.

Staff should not hold pupil information on personal devices or use personal devices to take and store images of pupils.

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. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate 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 academy events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment; the personal equipment of staff should not be used for such purposes and should be removed from school systems after two years.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy 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 pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The academy must ensure that:

- It has a Data Protection Policy. (see Life MAT website)
- 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 an 'information asset register' 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. The school should have 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. We have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals

- it provides staff, parents, volunteers, and older children with information about how the academy looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice on Life MAT website)
- 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.
- The Academy has a Freedom of Information Policy which sets out how it will deal with FOI requests. (see Life MAT website)
- 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 stored on the google drive which has two step verification enabled. • device must be password 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 academy policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safekeeping 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 the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- will not transfer any academy 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

- have locked their computers when not in direct use e.g. when they leave the room
- only use a computer in which they are logged in using their own school details, or are using a colleague’s login with their supervision and permission.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Staff	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Mobile phones may be brought to the academy	x			
Use of mobile phones in lessons		x		
Use of mobile phones in social time		x		
Taking photos on mobile phones/cameras Use of other mobile devices e.g. tablets, gaming devices		x		x
Use of personal email addresses in academy, or on academy network				x

Use of academy email for personal emails				x
--	--	--	--	---

Use of messaging apps		x		
Use of social media			x	
Use of blogs		x		

Pupils	Allowed	Allowed at certain times Allowed with staff permission/supervision	Not allowed
Mobile phones may be brought to the academy			x
Use of mobile phones in lessons			x
Use of mobile phones in social time			x
Taking photos on mobile phones/cameras Use of other mobile devices e.g. tablets, gaming devices		x	x
Use of personal email addresses in academy, or on academy network			x
Use of academy email for personal emails			x
Use of messaging apps			x

Use of social media		x	
---------------------	--	---	--

Use of blogs x

When using communication technologies, the academy considers the following as good practice: ● The official academy 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/academy email service to communicate with others when in school, or on school/academy systems (e.g. by remote access).

- Users must immediately report, to the nominated person – in accordance with the academy 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) academy systems. Personal email addresses, text messaging 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 will be provided with individual school/academy 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 academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs 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 the *school/academy* or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The academy 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

Academy staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or academy 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 *academy* or local authority/MAT ● Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official academy 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 (J Olsen and L Halford)
- A code of behaviour for users of the accounts,
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school/academy 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 the school/academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy 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 academy 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 has the settings to restrict parents and carers from commenting on posts made by the school administrator

The academy's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school/academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school/academy context, either because of the age of the users or the nature of those activities.

The academy believes that the activities referred to in the following section would be inappropriate in an academy context and that users, as defined below, should not engage in these activities in/or outside the academy when using academy equipment or systems. The academy policy restricts usage as follows:

Acceptable

Acceptable at

certain times

Acceptable for

nominated

users

Unacceptable

Unacceptable

Unacceptable

Unacceptable

Unacceptable

Unacceptable

Unacceptable

Users shall not visit

Internet

sites,

make,

post,

and

illegal

User Actions

Unacceptable

data
transfer, communicate or
pass on, material, remarks,
proposals or

download, upload,
comments that
contain or relate to:

-

-

-

-

Child sexual abuse images –The making
production or distribution of indecent images
of children. Contrary to The Protection
Children Act 1978

Grooming, incitement, arrangement of

X

facilitation of sexual acts against child
Contrary to the Sexual Offences Act

2003.

Possession of an extreme pornograph

X

image (grossly offensive, disgusting o
otherwise of an obscene character) C
to the Criminal Justice and Immigratio
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

Pornography

Promotion of any kind of discrimination

threatening behaviour, including promotion
of physical violence or mental harm

Promotion of extremism or terrorism

Any other information which may be
offensive to colleagues or breaches the
integrity of the ethos of the school or brings
the school into disrepute

that might be classed as cyber-crime under the
r Misuse Act:

aining unauthorised access to school networks,
ata and files, through the use of
omputers/devices

reating or propagating computer viruses or
ther harmful files

Revealing or publicising confidential or
roprietary information (e.g. financial / personal
formation, databases, computer / network
ccess codes and passwords)

isable/Impair/Disrupt network functionality
hrough the use of computers/devices

X

- Using penetration testing equipment (without
relevant permission)

Using systems, applications, websites or other
mechanisms that bypass the filtering or other
safeguards employed by the school/academy

On-line gaming (educational)

On-line gaming (non-educational)

On-line gambling

On-line shopping/commerce

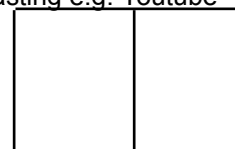
File sharing

Use of social media

Use of messaging apps

Use of video broadcasting e.g. Youtube

X



x	
	x
	x
	x
	x

	x
--	---

x

x

x

x

x

x

x

Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)

Unfair usage (downloading/uploading large files that hinders others in their use of the internet)

Using school systems to run a private business

Infringing copyright

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - offences under the Computer Misuse Act (see User Actions chart above)
 - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the academy 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/academy actions & sanctions

It is more likely that the academy 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/disciplinary procedures as follows:

Actions/Sanctions

Re			F
Incident	De	er	
ts	ut	pa	
fer	or	rt	
to	Re	m	
cla	fer	en	
ss	to	t/Y	
te	He	ea	
ac	ad	r/o	
he	of	th	

	Refer		t
	to		i
	technic al		o
	suppor t		n e .
	staff for		g
	action re		.
	filtering		d
	/securit y		e
	etc.	Re m	t
		u	e
		r	n
		t	t
	Inf or m	h	i
	pa re	e	o
Re	nt	r	n
fer to Po	s/c ar	s	/
lic	er	a	e
e	s	n	n
		c	

ov al of ne

Re tw or k/i nt x c l
 fer to He ad er ne t u s i
 te ac ce ss rig o
 ac ht
 he s
 r W ar ni
 ng

Pupils

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).

Unauthorised use of non-educational sites during lessons

Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device

X X X							
x							x
x					x		x

Unauthorised/inappropriate use of social media/ messaging apps/personal email

Unauthorised downloading or uploading of files

Allowing others to access academy network by sharing username and passwords

Attempting to access or accessing the academy network, using another pupil's account

Attempting to access or accessing the academy network, using the account of a member of staff

Corrupting or destroying the data of other users

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature

Continued infringements of the above, following previous warnings or sanctions

Actions which could bring the academy into disrepute or breach the integrity of the ethos of the school

Using proxy sites or other means to subvert the academy's filtering system

Accidentally accessing offensive or pornographic material and failing to report the incident

Deliberately accessing or trying to access offensive or pornographic material

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

				x	x			
x				x				

x				x	x		
x				x			
x		x		x	x		
x							
		x			x		
						x	
		x		x		x	
		x		xx		x	
x		x	x	x	x		
		x	x	x	x	x	

x x

Incident	Actions/Sanctions	
	Pri	action re
S	nci pal	filteri
Refer to lin		Warning
e	Refer to Lo	Suspensio
ma na	cal Au th	n
ger	ori ty/ HR	Disciplinary
Refer	Refer to	action
to	Police	
He	Refer to	
adt ea	Technical	
ch	Support	
er	Staff for	

Staff

Deliberately accessing or trying to access
Actions which could bring the school/academy
into disrepute or breach the integrity of the
ethos of the school/academy
ng
etc.

	X	X	X			
	x					
	x			x		
	x			x		

	x	x		x		
	x					
	x		x		x	x
	x					
	x					
	x					

material that could be considered illegal (see list
in earlier section on unsuitable/inappropriate
activities).

Inappropriate personal use of the internet/social

media/personal email

Unauthorised downloading or uploading of files

Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account

Careless use of personal data e.g. holding or transferring data in an insecure manner

Deliberate actions to breach data protection or network security rules

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature

Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils

Actions which could compromise the staff member's professional standing

Using proxy sites or other means to subvert the school's/academy's filtering system

Accidentally accessing offensive or pornographic material and failing to report the incident

Deliberately accessing or trying to access offensive or pornographic material

Breaching copyright or licensing regulations

Continued infringements of the above, following

	x					
--	---	--	--	--	--	--

	x					
	X					

previous warnings or sanctions

Appendix

	x					
--	---	--	--	--	--	--

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

[SWGfL Online Safety Policy Templates](#)

Acknowledgements

SWGfL would like to acknowledge the contribution of a wide range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of the online safety policy templates and of the 360 degree safe online safety self-review tool.

Copyright of these template policies is held by SWGfL. Schools/academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

This Policy has been signed by:

Position on Governing Body:

Date:

Review date: September 2022