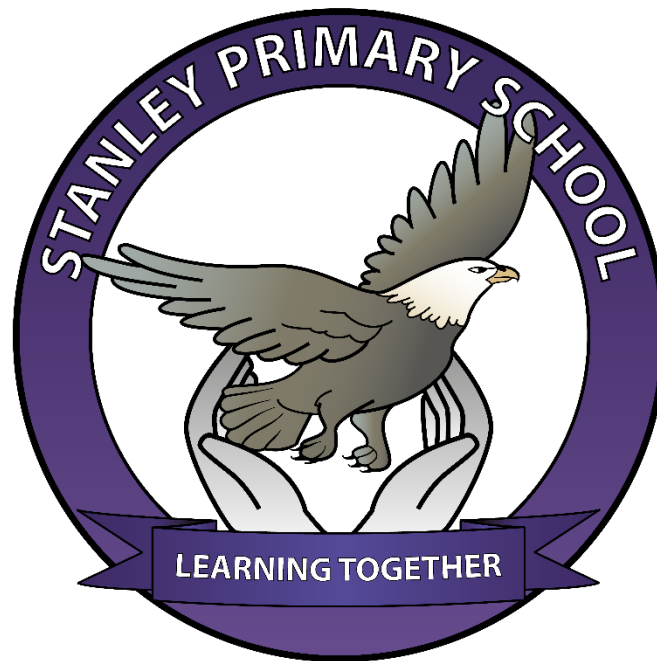


STANLEY PRIMARY SCHOOL



ONLINE SAFETY POLICY

Approved by:	Headteacher	Date: October 2010
Last reviewed on:	July 2023	
Next review due by:	July 2024	

SCOPE OF THE POLICY

This policy applies to all members of the school 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 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 Online 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 Online Safety behaviour that take place out of school.

The school will monitor the impact of this policy using:

- Logs of reported incidents
- Monitoring logs of internet activity/filtering
- Internal monitoring data of network activity
- Surveys of pupils, parents and staff

ROLES AND RESPONSIBILITIES

The following section outlines the online safety roles and responsibilities of individual and groups within school.

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

- Regular meetings with the computing coordinators and IT Administrator
- Regular monitoring of online safety incident logs

- Reporting to relevant Governors meetings

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 will be delegated to the Online Safety Coordinators.
- The headteacher and at least one other 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 “Responding to incidents of misuse” and relevant Local Authority HR disciplinary procedures).
- The headteacher is responsible for ensuring that the Online Safety Coordinator 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 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 headteacher will meet with the online safety team termly unless there is cause for concern, in which case the incident will be dealt with immediately.

Online Safety Team:

- Liaises with the Online Safety Governor and the school’s Senior Leadership Team to discuss current issues, review incident logs and filtering logs.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place. Any reported incidents concerning online safety will be dealt with appropriately and depending on the incident the most appropriate policy will be followed.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Attends relevant meetings with Governors

Technical Staff

The technical staff are 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 online safety technical requirements and any Local Authority online safety guidance that may apply
- That users may only access the networks and devices through a properly enforced password protection policy in which passwords are regularly changed
- Filtering is applied and updated on a regular basis
- They are up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update staff as relevant
- That the use of the network/internet/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Online Safety Coordinator for investigation/action/sanction
- That monitoring software and systems are implemented and updated as agreed in school policies
- Regular monitoring of filtering logs

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- They have read, understood and signed the Staff Acceptable Usage Policy
- They report any suspected misuse or problem to the Headteacher and Online Safety Coordinator for investigation/action/sanction
- All digital communications with pupils and parents/carers should be on a professional level and online 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 Policy and Acceptable Usage policy
- 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
- Cyber-bullying

Pupils

- Are responsible for using the school 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 cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/careers 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, the school website and information about nation/local online safety campaigns/literature.


Parents/carers will be encouraged to support the school 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's sections of the website
- 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 online safety is



therefore an essential part of the school's online safety provision. Children 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/PSHE/other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and teaching activities.
- Pupils should be taught in all relevant lessons to be critically aware of materials and content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the sources of information used and to respect copyright when using materials access 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 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 they visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drug use, discrimination) that would normally result in searched being blocks. In such a situation, staff can request that the

Technical Staff can temporarily removes those sites from the filtered list. 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 plan 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 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
- Newsletters and the school website
- Parent's evenings/sessions
- High profile events e.g Safer Internet Day
- Reference to the relevant websites e.g swgfl.org.uk / www.saferinternet.org.uk / www.childnet.com/parents-and-carers

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the school website and occasional briefings and courses as appropriate.

EDUCATION AND TRAINING - STAFF

It is essential that all staff receive online safety training and understand their responsibilities as outlined in this policy. All staff should be aware of safeguarding and child protection relating to online abuse and online sexual harassment.

ONLINE ABUSE

- **Grooming:** through social media and/or gaming, this may involve radicalisation and/or sexual abuse
- **Cyberbullying:** can occur through any device on and offline, especially mobile phones
- **Sexting:** sending explicit or compromising photos or videos
- **Sexual abuse:** including noncontact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways
- **Financial:** laundering money does happen to young people's bank accounts, online gambling is an increasing risk alongside inducements for sexual abuse while live streaming or in gaming

- **Exposure to inappropriate materials:** racial hatred, radicalisation, frightening or pornographic pictures and videos
- **Online addictions:** obsessive use of the internet and ICT, e.g. addiction to video games
- **Copyright infringement:** possession or sharing of illegally obtained music, pictures, videos or documents
- **Hacking:** children are becoming increasingly tech savvy and can sometimes find ways to circumvent cyber security measures put in place to protect themselves and others

ONLINE SEXUAL HARASSMENT

This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:

- consensual and non-consensual sharing of nude and semi-nude images and/or videos¹⁹. As set out in UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people (which provides detailed advice for schools and colleges) taking and sharing nude photographs of U18s is a criminal offence;
- sharing of unwanted explicit content;
- upskirting (is a criminal offence);
- sexualised online bullying;
- unwanted sexual comments and messages, including, on social media;
- sexual exploitation; coercion and threats.

It is important that schools and colleges consider sexual harassment in broad terms. Sexual harassment (as set out above) creates a culture that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence.

TRAINING – ONLINE SAFETY GOVERNORS

Governors should take part in online safety training with particular importance for those who are members of any subcommittee/group involved in technology/online safety/healthy and safety/safeguarding.

TECHNICAL – INFRASTRUCTURE/EQUIPMENT, FILTERING AND MONITORING

The school will be responsible for ensuring that the school infrastructure is as safe and secure as 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 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
- The master/administrator passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leaders and kept in a secure place.
- The IT Administrator 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 licenses purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content is filtered by the school's provider.
- Internet filtering should ensure that the children are safe from terrorist and extremist material when accessing the internet.
- An appropriate system is in place for users to report and actual/potential technical incident/security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (acceptable usage policy) for the provision of temporary access of guests (trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place (acceptable usage policy) that allows/forbids staff from installing programmes on school devices.

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

MOBILE TECHNOLOGIES

Mobile technology devices may be school owned/provided or personally owned and might include: smartphones, tablets, notebooks, laptops 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 of mobile devices in school context is educational. If staff or visitors have access to the school's network, they will comply with the school's Mobile Technologies Policy.

The school allows:

	School Devices		Personal Devices		
	School owned for single user	School owned for multiple user	Pupil owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes (kept in office)	Yes	Yes
Full network access	Yes	Yes	No	No	No
Internet only				Yes- Occasional	Yes – Occasional
No network access			Yes	Yes - Occasional	Yes - Occasional
Smart devices e.g. Smart watches			No	Yes	Yes

Personal Devices

- Staff must comply with the Acceptable Usage Policy and Mobile Technologies Policy.
- Staff will be allowed to use personal devices for school business, such as emails.
- No technical support will be provided by the school for personal mobile devices
- No personal devices can be connected to the schools servers
- The school has the right to take, examine and search devices belonging to school in the case of misuse.
- No personal devices will be used to take images or videos of children in or out of school
- The owner is responsible for any loss, damage or malfunction of personal devices in school
- Visitors will be supervised and monitored and should only use personal devices with permission and prior approval

Use of digital and video images

The development of digital image 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 and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-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 long 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 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or seesaw.
- Parents are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publically available on social networking sites, nor should parents comment on any activities involving other pupils in the digital images and videos.
- Staff and volunteers are allowed to take digital/video images to support education aims but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website or seesaw will be selected carefully and will comply with good practice guidance on the use of such images.

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:	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 or extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
	Infringing copyright				X	
	Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
	Creating or propagating computer viruses or other harmful files				X	
	Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
	Online gaming (educational)	X				
	Online gaming (non-educational)				X	
	Online gambling				X	

Online shopping/commerce		x			
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. youtube		x			

- Care should be taken when Publishing pupils' names on a website or seesaw, particularly in association with photographs.
- Pupils work can only be published with the permission of the pupil and parents or carers.

DATA PROTECTION

School will follow and is aware of the importance of the Data Protection Act 1998 and other relevant legislation.

UNSUITABLE/INAPPROPRIATE ACTIVITIES USING SCHOOL EQUIPMENT:

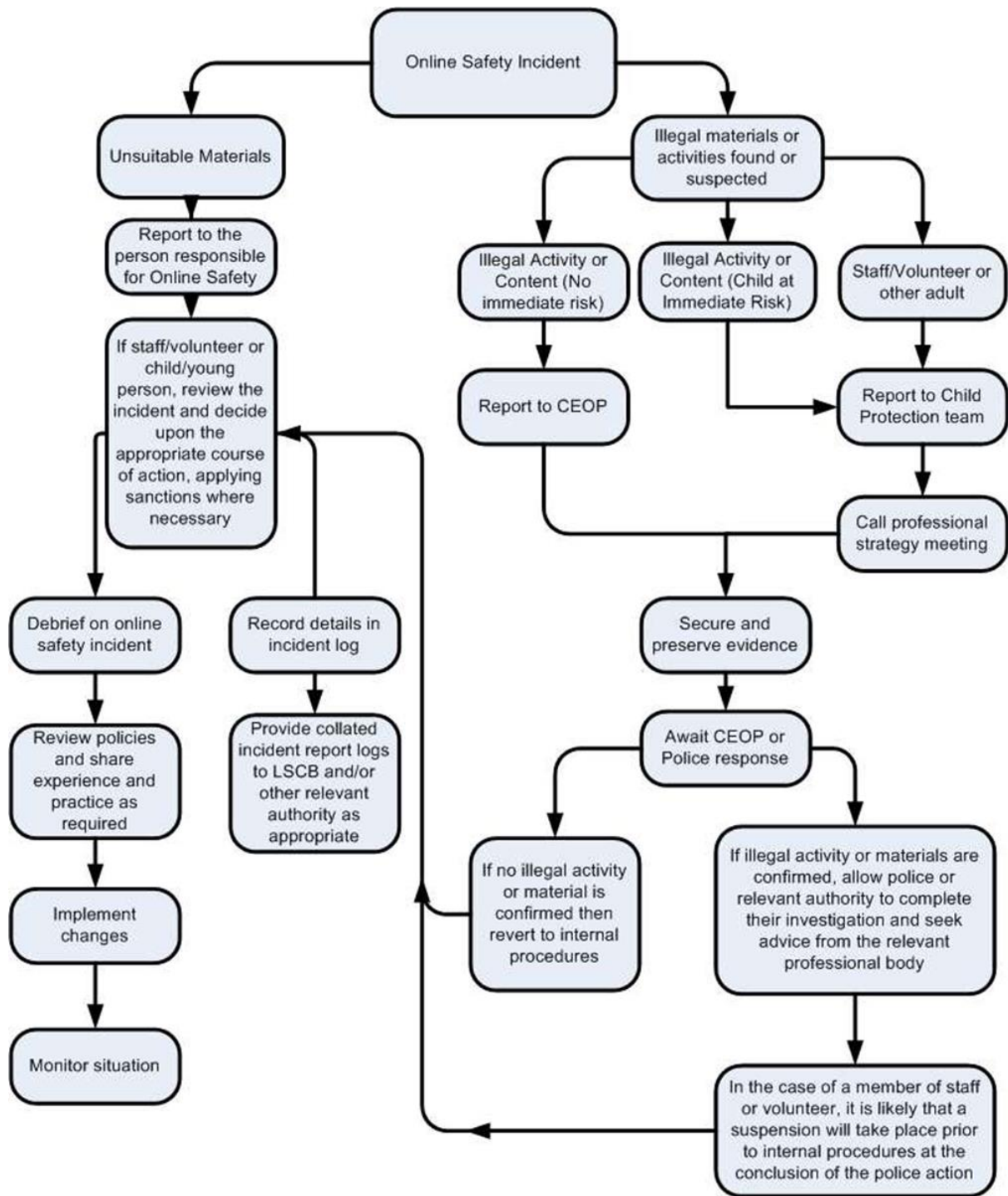
Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in or outside the school when using school equipment or systems. The school policy restricts usage as follows:

RESPONDING TO THE INCIDENTS OF MISUSE

This guidance is intended for 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 table above).


ILLEGAL INCIDENTS

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, inform the appropriate designated person who will take the appropriate action using the flowchart below as guidance.



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. Any incidents will be appropriately investigated by the designated person on school and further advice will be taken as appropriate.

SCHOOL ACTIONS AND 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 / disciplinary procedures.