Park Road Academy Primary School

e-Safety including Social Media Policy
2025 - 2026

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 cyberbullying, or other eSafety 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 Management 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 eSafety behaviour that take place out of school.

Roles and Responsibilities

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

Governors:

The Governing Body will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Designated Safeguarding Lead's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.

- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.

- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

Headteacher (Miss K Hart):

- The Headteacher has a duty of care for ensuring the safety (including eSafety) of members of the school community, though the day-to-day responsibility for eSafety will be delegated to the eSafety Co-ordinator.

- The Headteacher; K Hart (Trained Designated Safeguarding Lead), L Taylor and S Breen (Designated Safeguarding Leads) and L Harrison (Deputy Designated Safeguarding Lead) are aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff.

- The Headteacher is responsible for ensuring that the eSafety Coordinator (T Smart) and other relevant staff receive suitable training to enable them to carry out their eSafety 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 eSafety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Headteacher will receive regular monitoring updates from the eSafety Co-ordinator.

eSafety Coordinator (Mr T Smart):

- takes day-to-day responsibility for eSafety issues and has a leading role in establishing and reviewing the school eSafety policy and reports regularly to the Headteacher.

- ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.

- provides training and advice for staff.

- liaises with the relevant bodies e.g. CEOP, Trafford Local Authority, Infinity Computing
- liaises with school network technicians (S Brannan – Infinity Computing)
- receives reports of eSafety incidents and creates a log of incidents to inform future eSafety developments.
- meets regularly with Governors to discuss current issues, review incident logs and filtering / change control logs.

Technical staff:

The Computing Subject Lead (T Smart) and ICT Support Technicians (S Brannan) 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 eSafety technical requirements and any Local Authority (LA) 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.
- that they keep up to date with eSafety technical information in order to effectively carry out their eSafety roles and to inform and update others as relevant.
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation.
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:

Teaching and support staff are responsible for ensuring that:

- they have an up-to-date awareness of eSafety matters and of the current school eSafety Policy and practices.

- they have read, understood and signed the Staff Acceptable Use Policy.
- they report any suspected misuse or problem to the Headteacher/eSafety Coordinator for investigation.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems.
- eSafety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the eSafety Pledge and Acceptable Use Agreement.
- 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 taught how to ensure that their internet searches are suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Leads:

The Designated Safeguarding Lead will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.

- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.

- Understanding the filtering and monitoring processes in place at the school.

- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.

- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.

- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement and Pupil eSafety Pledge.

- 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 eSafety practice when using digital technologies out of school and realise that the school's eSafety 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 information evenings, newsletters, websites and information about relevant eSafety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good eSafety practice and to follow guidelines on the appropriate uses of:

- digital and video images taken at school events.
- their children's personal devices in the school (where this is allowed).

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, useage must be balanced by educating pupils to take a responsible approach. The education of pupils in eSafety is therefore an essential part of the school's eSafety provision.

Children and young people need the help and support of the school to recognise and avoid eSafety risks and build their resilience. eSafety is a focus in all areas of the curriculum and staff reinforce eSafety messages across the curriculum. The eSafety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned eSafety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited.
- Key eSafety messages are reinforced as part of a planned programme of assemblies and whole school events, such as Safer Internet Day.
- 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.
- 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. Children are also taught how to search for information that is relevant and appropriate for their age group.

Education - Digital Well-being and Mental Health

Embedding Digital Well-being into the Curriculum:

- Awareness Building: Pupils will learn about the impact of excessive screen time, the effects of social media on mental health, and strategies to maintain a healthy digital balance.

- PSHE Integration: The PSHE curriculum will include topics on cyberbullying, online relationships, and resilience against digital stressors.

Education – Parents / Carers

Parents and carers may have only a limited understanding of eSafety 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:

- Appropriate information web sites (e.g. www.thinkyouknow.co.uk)

- Information evenings / high profile events / campaigns e.g. Safer Internet Day, NSPCC workshop

Education – The Wider Community

The school will provide opportunities for members of the local community to gain from the school's eSafety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and eSafety.

- eSafety messages targeted towards grandparents and other relatives as well as parents.

- The school website provides eSafety information for the wider community.

- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their eSafety provisions.

Education & Training – Staff / Volunteers

The Designated Safeguarding Lead will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Training will be offered as follows:

- A planned programme of formal eSafety training is compulsory for all staff. This will be regularly updated and reinforced. An audit of the eSafety training needs of all staff will be carried out annually.

- All new staff will receive eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety Policy and Acceptable Use Agreements.

- The eSafety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

- This eSafety policy and its updates will be presented to and discussed by staff in staff meetings.

- The eSafety Coordinator will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

Incident Reporting and Response

Flowchart for Responding to Online Safety Incidents The existing flowchart for handling incidents will be visually updated for clarity. It will emphasise:

Immediate Reporting: Staff and pupils must report concerns immediately to the eSafety Coordinator or Filtering and Monitoring Team.

Escalation Path: Incidents involving illegal activity will be reported directly to CEOP or the police.

Clear Steps for Staff: Specific guidance will outline how staff should document incidents while maintaining confidentiality.

Enhanced Log Automation: A secure digital solution will be implemented for logging and tracking incidents, ensuring anonymised and centralised data.

The Filtering and Monitoring Team will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges. The Filtering and Monitoring Team will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Designated Safeguarding Lead will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their eSafety 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 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.
- 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. Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by Trafford. Content lists are regularly

updated and internet use is regularly monitored. There is a clear process in place to deal with requests for filtering changes.

- 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 / potential technical incident / security breach to the relevant person (T Smart, S Breen and L Taylor), 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 (staff / pupils / community users) are allowed on school devices that may be used out of school.

- An agreed policy is in place that allows staff to download executable files and install 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.

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 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).

- 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 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 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 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, unless express parental permission has been sought beforehand.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (covered as part of the GDPR agreement signed by parents or carers at the start of the year).

Data Protection

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.

- Collected for specified, explicit and legitimate purposes and not further processed in a

manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, Insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. 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. An encrypted email service for the sharing of personal information outside of the school system is available to staff.

- 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, chat, 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 eSafety 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.

- Pupils in Upper Key Stage 2 will be provided with individual school email addresses for educational use after parental consent has been obtained.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Online Safety and AI – DfE Guidance

The Department for Education's 2025 policy on generative AI in education highlights the importance of embedding online safety principles within digital tool usage in schools. In response, Park Road Academy is adopting the following updates to its eSafety and Social Media Policy:

• Any use of generative AI tools (e.g. ChatGPT, Microsoft Copilot, Google Gemini) must follow the school's Acceptable Use Policy and must not expose pupils to unsafe, biased, or unverified content.

• Generative AI tools are not to be used by pupils except under structured, teacher-led activities with appropriate safeguards and filtering in place.

• Staff must not input personal, identifiable, or sensitive pupil information into AI platforms.

• Pupils will receive additional education through PSHE and Computing on the risks associated with AI-generated misinformation and online impersonation.

• Online safety lessons will incorporate guidance on identifying AI-generated content and verifying authenticity of online sources.

• The Designated Safeguarding Lead (DSL) will monitor any emerging threats arising from AI misuse and ensure that incidents are logged and responded to appropriately.

• Social media guidance is updated to include warnings against AI-generated chatbots or

content designed to mislead or manipulate children.

Social Media

Park Road Academy Primary school is aware and acknowledges that increasing numbers of adults and children are using Social Media sites.

The widespread availability and use of Social Media applications bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly.

This policy and associated guidance is to protect staff and advise school leadership on how to deal with potential inappropriate use of Social Media sites. For example, our use of Social Media applications has implications for our duty to safeguard children, young people and vulnerable adults. The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice.

This policy covers the use of Social Media applications by all school stakeholders, including, employees, Governors and pupils. These groups are referred to collectively as 'school representatives' for brevity.

The requirements of this policy apply to all uses of Social Media applications which are used for any school related purpose and regardless of whether the school representatives are contributing in an official capacity to Social Media applications provided by external organisations.

Social Media applications include, but are not limited to:

- Blogs, for example Blogger
- X (formerly known as Twitter)
- Online discussion forums, such as netmums.com and collaborative spaces
- Media sharing services, for example YouTube, Facebook.

All school representatives should bear in mind that information they share through Social Media applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Equality and Diversity Policy.

Social Media Guidance and Advice

Employees who choose to make use of private Social Media sites / applications should be advised as follows:

(i) That they should not access these sites for personal use during working hours;

(ii) That they familiarise themselves with the site's 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended;

(iii) That they do not associate their Social Media presence directly with their school employment.

Social Media Applications

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.

- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns - in relation to the school's own media platforms not personal platforms.

- Must not be used in an abusive or hateful manner.

- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.

- Must not breach the school's misconduct, equal opportunities or bullying and harassment policies.

- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents.

- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with.

- Employees should not identify themselves as a representative of the school.

- References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Headteacher.

- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.

Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

Guidance/Protection for Staff on using Social Media

- No member of staff should interact with any pupil in the school on Social Media sites.
- No member of staff should interact with any ex-pupil in the school on Social Media sites who is under the age of 18.
- This means that no member of the school staff should request access to a pupil's area on the Social Media site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.
- Where family and friends have pupils in school and there are legitimate family links, please inform The Headteacher, in writing.
- It is illegal for an adult to network, giving their age and status as a child.

Guidance/Protection for Pupils on using Social Media

- No pupil under 13 should be accessing Social Media sites.
- No pupil may access Social Media sites during the school working day.
- No pupil should attempt to join a staff member's areas on Social Media sites. If pupils attempt to do this, the member of staff is to inform the Headteacher. Parents will be informed if this happens.
- Any attempts to breach firewalls will result in a ban from using school ICT equipment other than with close supervision.
- Please report any improper contact or cyber bullying to your class teacher in confidence as soon as it happens.
- We have a zero tolerance to cyber bullying.

Guidance/Protection for Parents on using Social Media

Please refer to the school's Parents' Social Media Code of Conduct (available on the school website).

Child Protection Guidance

If the Headteacher receives a disclosure that an adult employed by the school is using a Social Media site in an inappropriate manner as detailed above, they should:

- Record the disclosure in line with the School's Child Protection Policy
- Schools must refer the matter to the LA who will investigate.
- If the disclosure has come from a parent, take normal steps to calm the parent and explain processes.
- If disclosure comes from a member of staff, try to maintain confidentiality.
- The LA and the Trust will advise whether the member of staff should be suspended pending investigation, after contact with the police. It is not recommended that action is taken until advice has been given.
- If disclosure is from a child, follow your normal process in the School's Child Protection Policy until the police investigation has been carried out.

Protecting Professional Identity

All schools, academies and LAs have a duty of care to provide a safe learning environment for pupils and staff. Schools and LAs 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 LA 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 limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions, Risk assessment, including legal risk School staff should ensure that:
- No reference should be made in social media to 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. The school's use of social media for professional purposes will be checked regularly by the e-safety coordinator.

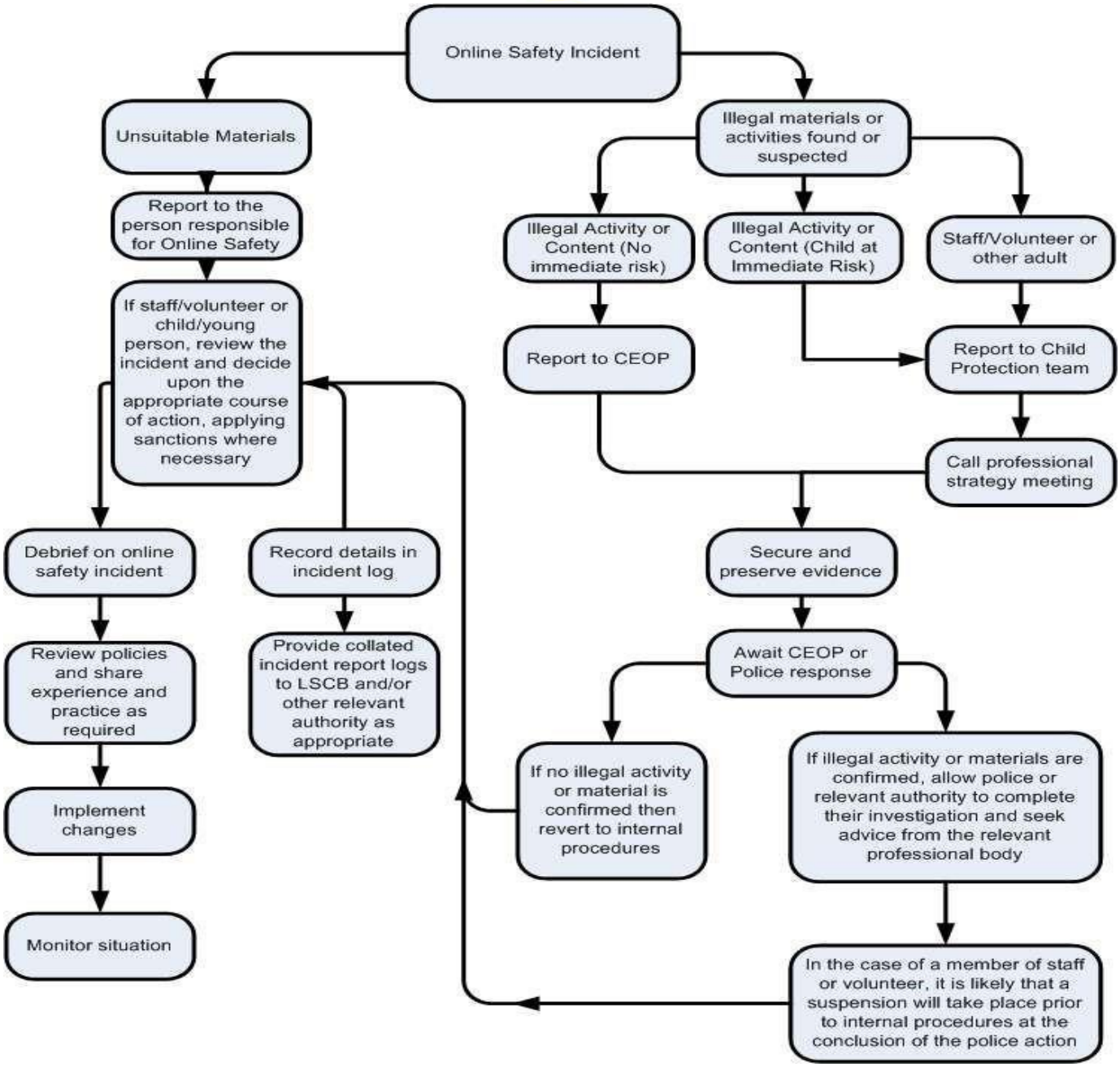
Unsuitable / inappropriate activities

Some internet activity (e.g. accessing child abuse images or distributing racist material) is illegal and would obviously be banned from school and all other technical systems. Other activities (e.g. cyberbullying) 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: **User Actions**	Acceptable	Acceptableatcertaintimes	Acceptablefornominated users	Unacceptable	Unacceptableandillegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978				X	X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.				X	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	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	X
Pornography				X	X
Promotion of any kind of discrimination				X	X
Threatening behaviour, including promotion of physical violence or mental harm				X	X

Promotion of extremism or terrorism				X	X
Using school systems to run a private business				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 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 (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media		X			
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube			X		

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 for responding to online safety incidents and report immediately to the police.



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 / disciplinary procedures.

Schedule for Monitoring & Review

The implementation of this eSafety policy will be monitored by the:	Computing Lead (T Smart)
Monitoring will take place at regular intervals:	Annually
The Governing Body will receive a report on the implementation of the eSafety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The eSafety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2026
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Trafford Safeguarding Officer, Greater Manchester Police, CEOP

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