YSGOL GYNRADD

PARC LEWIS

PRIMARY SCHOOL

E-Safety Policy

Audit as per LEA Policy Document guidance	
Checked by	**date**
Approved by	**date**
Date of Next Review:	

This policy applies to all members of the school community (including staff, pupils, volunteers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

Introduction

School e-Safety Policy

Development, monitoring and review of the Policy

Schedule for development, monitoring and review

Roles and Responsibilities

- Governors
- Headteacher and Senior Leaders
- e-Safety Co-ordinator
- Network Manager / Technical Staff
- Teaching and Support Staff
- Safeguarding Designated Person
- E-Safety Group
- Pupils
- Parents / Guardians

Policy Statements

- Education –Pupils
- Education – Parents / Guardians
- Education – The Wider Community
- Education and training – Staff / Volunteers
- Training – Governors
- Technical – infrastructure / equipment, filtering and monitoring
- Use of digital and video images
- Data protection
- Communications
- Social Media - Protecting Professional Identity
- User Actions - unsuitable / inappropriate activities
- Responding to incidents of misuse
- Passwords

Development / Monitoring / Review of this Policy

This e-Safety policy has been developed by a working group at Parc Lewis Primary made up of:

- *Headteacher*
- *Senior Leaders*
- *e-Safety Coordinator*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the *Governing Body / Governors Sub Committee on:*	*May 2017*
The implementation of this e-Safety policy will be monitored by the:	*Head teacher and senior leadership team*
Monitoring will take place at regular intervals:	*At least once a year*
The *Governing Body* will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-Safety incidents) at regular intervals:	*once a year*
The e-Safety 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 e-Safety or incidents that have taken place. The next anticipated review date will be:	*May 2018*
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, Police, TCBC*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of
  - pupils
  - parents / Guardians
  - staff

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing body receiving regular information about e-Safety incidents and monitoring reports. The e-Safety Governor's role includes:

- regular meetings with the e-Safety Co-ordinator
- regular monitoring of e-Safety incident logs
- regular monitoring of filtering / change control logs (where possible)
- reporting to relevant Governors / sub-committee / meeting

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-Safety) of members of the school community, though the day to day responsibility for e-Safety is delegated to the e-Safety Co-ordinator
- The Headteacher and (at least) another member of the Senior Leadership Team is aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff
- The Headteacher and Senior Leaders are responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-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 e-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Senior Leadership Team will receive regular monitoring reports from the e-Safety Co-ordinator

E-Safety Coordinator:

The e-Safety Coordinator

- leads the e-Safety committee
- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place
- provides (or identifies sources of) training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with technical staff
- receives reports of e-Safety incidents[1] and creates a log of incidents to inform future e-Safety developments
- meets regularly with e-Safety Governor to discuss current issues, review incident logs and if possible, filtering / change control logs
- attends relevant meeting / sub-committee of Governors

- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

NOTE: The school has a managed ICT service provided by RCT, although we acknowledge that it is the responsibility of the school to ensure that the managed service provider carries out all the e-Safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school e-Safety policy and procedures.

The Network Manager / Technical Staff (or managed service provider) is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the required e-Safety technical requirements as identified by the Local Authority or other relevant body and also the e-Safety Policy / 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
- that the filtering policy, is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- that they keep up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the Head teacher, Senior Leader Team; e-Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher Senior Leader Team ; e-Safety Coordinator for investigation / action
- all digital communications with students / pupils / parents / Guardians should be on a professional level
- e-Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-Safety and acceptable use agreements
- 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

Safeguarding Designated Person

NOTE: It is important to emphasise that these are safeguarding **issues,** not technical issues; the technology provides additional means for safeguarding issues.

The Safeguarding Designated Person is trained in e-Safety issues and is aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Group

The e-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-Safety and monitoring the e-Safety policy including the impact of initiatives. The group is responsible for regular reporting to the Governing Body.

Members of the e-Safety Group will assist the e-Safety Coordinator with:

- the production / review / monitoring of the school e-Safety policy / documents
- mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs where possible
- consulting stakeholders – including parents / Guardians and the pupils about the e-Safety provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self-review tool

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Guardians

Parents / Guardians play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-Safety campaigns / literature. Parents and Guardians will be encouraged to support the school in promoting good e-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 / VLE and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

Policy Statements

Education – Pupils

The education of pupils in e-Safety is an essential part of the school's e-Safety provision. Children and young people need the help and support of the school to recognise and avoid e-Safety risks and build their resilience.

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

- A planned e-Safety curriculum is provided as part of ICT / Computing / PSE / Digital Literacy lessons or other lessons and should be regularly revisited
- Key e-Safety messages are 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 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
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites pupils 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 / Guardians

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 Guardians through

- Curriculum activities
- Twitter
- Letters, newsletters, web site, VLE
- Parents / Guardians evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. https://hwb.wales.gov.uk/ www.saferinternet.org.uk/ http://www.childnet.com/parents-and-Guardians

Education – The Wider Community

Where possible the school will provide opportunities for local community groups / members of the community to gain from the school's e-Safety knowledge and experience.

Education & Training – Staff / Volunteers

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

- A planned programme of formal e-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-Safety training needs of all staff will be carried out regularly
- All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Agreements
- The e-Safety Coordinator will receive regular updates through attendance at external training events (e.g. from Consortium / SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- This e-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days
- The e-Safety Coordinator will provide advice / guidance / training to individuals as required

Training – Governors

Governors will take part in e-Safety training / awareness sessions.

Technical – infrastructure / equipment, filtering and monitoring

The school has a managed ICT service provided by an outside contractor, although it is the responsibility of the school to ensure that the managed service provider carries out all the e-Safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school e-Safety Policy / Acceptable Use Agreements. The school should also check their Local Authority / other relevant body policies on these technical issues if the service is not provided by the Authority. School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

There will be regular reviews and audits of the safety and security of school technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- All users will be provided with a username and secure password by Rhondda Cynon Taff who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be advised to change their password every Term. Supply teachers will be given a supply username and password to access computer and registers
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- Parc Lewis Staff are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- The school has provided enhanced / differentiated user-level. Where possible, 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, 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 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 / Guardians and pupils need to be aware of the risks associated with publishing digital images on the internet. 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
- Parents / Guardians are welcome to take videos and digital images of their children at school events for their own personal use. Parents/Guardians are asked not to post images (photos and videos) of pupils other than their own children on social media sites unless they have the permission of parents of other children pictured
- Staff 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. Staff can use personal devices to upload to school social media and for class work but images should not be stored on any device and must be deleted
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or Guardians will be obtained before photographs of pupils are published. This will take the form of a permission letter when they join the school

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing

- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office

Staff must ensure that they:

At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices
- Store documents on a protected server or encrypted memory stick

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 & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	lowed for selected staff	Not allowed	Allowed	Allowed at certain times	ed with staff permission	Not allowed
Mobile phones may be brought to school	●						●	
Use of mobile phones in lessons		●						●

Use of mobile phones in social time	●							●
Taking photos on mobile phones / cameras			●					●
Use of other mobile devices e.g. tablets, gaming devices		●					●	
Use of personal email addresses in school, or on school network	●							●
Use of school email for personal emails				●				●
Use of messaging apps		●						●
Use of social media		●					●	
Use of blogs	●						●	

When using communication technologies the school considers the following as good practice:

- The official school email service and hwb emails 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 and hwb email service to communicate with others when in school, or on school systems (e.g. by remote access)
- Users must immediately report to the nominated person – in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and pupils or parents / Guardians (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Social Media

Social media sites play an important role in the lives of many people, including children. We recognise that social networking can bring many benefits, but there are also potential risks. The aim of this document is to give clarity to the way in which social media sites are to be used by the Parc Lewis School community: pupils, staff, parents, Guardians, governors and other volunteers. All members of the school community should bear in mind that information they share through social media and networks, even if it is on private spaces, is still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006, and UK libel and defamation laws.

A. The use of social media sites by pupils whilst at school

Pupils can tweet work onto the school Twitter page with permission and supervision from a teacher.

Pupils should not access social networking sites whilst at school. Pupils and parents will be reminded that the use of some social media sites is inappropriate for Primary-aged pupils.

Pupils do not use personal technology in school and do not take home school computing systems.

B. Use of social media sites by employees in a personal capacity

It is possible that a high proportion of staff will have their own social networking accounts. It is important that they protect their professional reputation, and that of the school, by ensuring that they use their personal sites in an appropriate manner.

Staff will be advised as follows:

That they familiarise themselves with social network sites' privacy settings in order to ensure that information is not automatically shared with a wider audience than intended. It is recommended that, as a minimum, all privacy settings are set to 'friends only', irrespective of use/purpose.

· That they do not conduct or portray themselves, or allow friends to portray them, in a manner which may:

- Bring the school into disrepute

- Lead to valid parental complaints

- Be deemed as derogatory towards the school and/or its employees

- Be deemed as derogatory towards pupils, parents/Guardians or governors

- Bring into question their appropriateness to work with children

- Contravene current National Teacher Standards

· They should not use their social media accounts during teaching time

- They should not interact on social media during the school day e.g. comments or likes

· That we advise them not to form online friendships or enter into communication with parents/Guardians as this could lead to professional relationships being compromised

· That they do not form online friendships or enter into online communication with pupils as this could lead to professional relationships being compromised, and/or safeguarding allegations being raised

· That they should not post pictures of or negative comments about school events

· That if their use of social media/networking sites contravenes this policy, they may be subject to Local Authority disciplinary procedures

Inappropriate use by employees should be referred to the Headteacher in the first instance.

C. Creation of social media accounts by school staff for use in education

All social media services must be approved by the Headteacher in advance of any educational work being undertaken.

D. Comments posted by parents/Guardians on social media sites

Parents/Guardians will be made aware of their responsibilities regarding their use of social media via this policy, the school Twitter account and school newsletters.

· Parents/Guardians are asked not to post images (photos and videos) of pupils other than their own children on social media sites unless they have the permission of parents of other children pictured

· Parents/Guardians are asked to raise queries, concerns or complaints directly with the school rather than posting them on social media

· Parents/Guardians should not post malicious or fictitious comments on social media sites about any member of the school community

E. Dealing with incidents of online (cyber) bullying

All cases of online bullying will be dealt with in accordance with the school's Anti-Bullying policy. The school can take action with reference to any incident that takes place outside school hours if it:

· Could have repercussions for the orderly running of the school

· Poses a threat to a member of the school community

· Could adversely affect the reputation of the school, or its employees/governors

Where appropriate, legal action will be taken by the school's governors.

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. cyber-bullying would be banned and could lead to criminal prosecution.

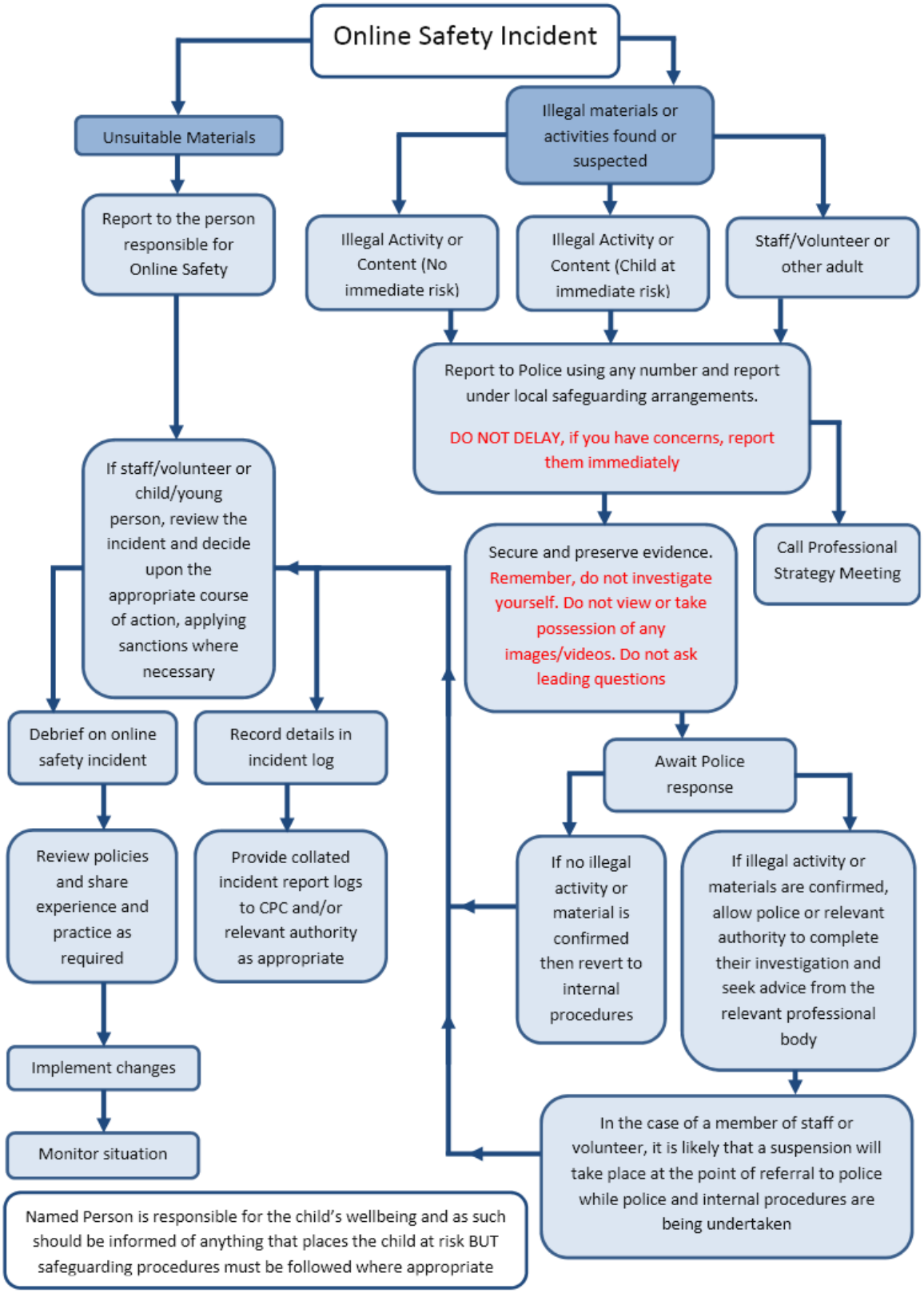
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at	Acceptable for nominate	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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					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 below for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have concerns, report them immediately
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence. Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions
Call Professional Strategy Meeting
Debrief on online safety incident
Record details in incident log
Await Police response
Review policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police while police and internal procedures are being undertaken
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT safeguarding procedures must be followed where appropriate

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

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

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

School Actions

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 as follows:

Procedures to follow when dealing with e-safety issues - pupils

- **Pupils**
- **Actions**

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / Guardians	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	x							x	x
Unauthorised use of mobile phone / digital camera / other mobile device	x	x						x	x
Unauthorised use of social media / messaging apps / personal email	x	x						x	X
Unauthorised downloading or uploading of files	x	x						x	X
Allowing others to access school network by sharing username and passwords	x	x	x		x	x		x	x
Attempting to access or accessing the school network, using another student's / pupil's account	x	x	X		x	x		x	x
Attempting to access or accessing the school network, using the account of a member of staff	x	x	x		x	x		x	x
Corrupting or destroying the data of other users	x	x	x		x	x		x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x		x	x		x	x
Continued infringements of the above, following previous warnings or sanctions	x	x	x		x	x	x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x	x		x	x	x	x	x
Using proxy sites or other means to subvert the school's 's filtering system	x	x	x		x	x	x	x	x

Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x		x	x	x	x	x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x	x
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

Procedures to follow when dealing with e-safety issues – Staff

- **Staff**
- **Actions**

Incidents:	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		x				x		
Unauthorised downloading or uploading of files		x			x	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		x			x	x		x
Careless use of personal data e.g. holding or transferring data in an insecure manner		x				x		
Deliberate actions to breach data protection or network security rules		x			x	x		x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x		x	x	x		x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x			x		x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x	x		x	x		x

Actions which could compromise the staff member's professional standing		x	x		x	x		x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x	x		x	x		x
Using proxy sites or other means to subvert the school's 's filtering system		x	x		x	x		x
Accidentally accessing offensive or pornographic material and failing to report the incident		x	x		x	x		x
Deliberately accessing or trying to access offensive or pornographic material		x	x	x	x	x		x
Breaching copyright or licensing regulations		x	x		x	x		x
Continued infringements of the above, following previous warnings or sanctions		x	x		x	x	x	x

Password Security

Policy Statements:

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the e-Safety Committee
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "master / administrator" passwords for the school systems, used by the technical staff must be kept in a secure place e.g. school safe
- All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Users will be advised to change their passwords every term

Staff passwords:

- All staff users will be provided with a username and password by the e-safety co-ordinator who will keep an up to date record of users and their usernames
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- For best practice, passwords should be changed at least every term, should not be re-used for 6 months and be significantly different from previous passwords created by the same user - the last four passwords should not be re-used
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of school
- a password is available for supply teachers to access SIMS

- Secure Envoy is used to generate a new password every time Sims is accessed outside of school
- Staff are advised for passwords to consist of numbers, uppercase letters, lowercase letters and symbols