

West Monmouth School

Ysgol Gorllewin Mynwy



E-Safety Policy

Polisi Diogelwch e

Date Approved by Governors:

Date Reviewed by Governors: Nov 2023

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the on:	
The implementation of this e-safety policy will be monitored by the:	e-safety group
Monitoring will take place at regular intervals:	Annually
The <i>Governing Body</i> 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:	Annually
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:	Nov 2024
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, Police Liaison Officer

The school will monitor the impact of the policy using:

- Logs of reported incidents from programs including Senso and HWB
- Periodic monitoring logs of internet activity (including sites visited)

Scope of the Policy

This policy applies to all members of the school community (including staff, students / 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 e-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 (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the School 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 e-safety behaviour that take place out of school.

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 annual information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety. The role of the E-Safety Governor will include:

- meeting with the E-Safety Co-ordinator / Officer
- monitoring of e-safety incident logs
- reporting to relevant Governors meeting

Headteacher:

- 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 will be delegated to the E-Safety Officer (Mr D Goodliffe)
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section)
- The Headteacher is responsible for ensuring that the E-Safety Officer, Data protection officer 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 Senior Leadership Team will receive regular monitoring reports from the E-Safety Officer.

E-Safety Officer:

- leads the e-safety group
- 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 training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets with E-Safety Governor to discuss current issues and review incident logs
- attends relevant meeting of Governing Body
- reports regularly to Senior Leadership Team

Data protection officer:

- Providing advice and guidance when required
- Creating and maintaining data records
- Drafting data policies and procedures
- Providing training for employees
- Acting as the first point of contact with authorities
- Managing Subject Access Requests and those under Freedom of Information Act
- Conducting an annual audit of data processes

: Network Manager:

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority 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
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person)
- that they keep up to date with 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 system is regularly monitored in order that any misuse / attempted misuse can be reported to E-Safety Officer and senior leader with overview of ICT strategy for investigation / action / sanction

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 Agreement (AUP)
- they report any suspected misuse or problem to E-Safety Officer
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are considered within the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils are made aware 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

Designated Safeguarding Officer

should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- 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 the monitoring the e-safety policy including the impact of initiatives.

Members of the E-safety Group will assist the E-Safety Officer with:

- the production / review / monitoring of the school e-safety policy / documents.
- reviewing the e-safety curricular provision
- monitoring network / internet / incident logs
- consulting stakeholders about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy Agreement. **This covers such things as:** Being responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use as set out in the 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, and be aware of the hazards involved with 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 / Carers

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

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 e-safety is therefore 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 across the curriculum and staff should reinforce e-safety messages as applicable. The e-safety provision may be provided in a number of ways:

- as part of PHSE and other lessons
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / 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 student / 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 students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's 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:

- Letters, newsletters, web site
- Parents evenings
- High profile events / campaigns eg Safer Internet Day
- Reference to relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/
<http://www.childnet.com/parents-and-carers>

Education & Training – Staff / Volunteers

Staff should receive e-safety training and understand their responsibilities as outlined in this policy. Training will be offered as follows:

- e-safety training will be made available to staff. And an audit of the e-safety training needs of all staff will be carried out regularly.
- The E-Safety Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / EAS 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 Officer will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school, in conjunction with the SRS 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 e-safety responsibilities

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by Mr A Davies 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 required to change their password periodically.
- 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 (eg school safe)
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- The school has provided enhanced / differentiated user-level filtering
- School technical staff monitor and may record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- 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” (eg trainee teachers, supply teachers, visitors) onto the school systems.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school’s normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Pupils receive guidance on the use of personal devices
- Any device loss, theft, change of ownership of the device will be reported

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 students / 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 eg on social networking sites.
- 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. [DG(MS1)]
- 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 students / 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Permission letters are stored within the pupils’ own school file. All permissions are recorded on SIMS, with a ‘No Photograph’ list available to all staff.
- Pupil’s work can only be published with the permission of the pupil and parents or carers.

Data Protection

New data protection legislation, the General Data Protection Regulation (“GDPR”) came into effect on 25 May 2018. This is supplemented by a new UK Data Protection Act. Among the changes made by GDPR is a requirement to have more detailed contracts where one organisation processes personal data on behalf of another

The school must ensure that:

- The Senior management team fully understand GDPR and its potential impact.
 - Review all of the personal data they hold; including data for pupils, staff, parents, suppliers and governors which should be organised and stored in an audit.
 - Consider the personal data processed and ensure everyone understands how it is collected, where it came from, what it is used for and what risks are posed by its use.
 - All staff are trained according to their roles and responsibilities. This should include general GDPR awareness training for all staff as well as more detailed training for staff with more responsibility (e.g. Head Teacher, Deputy Head Teacher, Data Protection Officer).
 - Assign a Data Protection Officer (DPO) who is solely responsible for any data protection and compliance with the GDPR regulation. It is important to consider where this role will sit in line with the school’s structure and governance arrangements
-
- If the data on any device is breached it must be reported Senior Leadership Team and DPO.
 - Where personal data is transferred outside the secure school network, it must be encrypted.
 - Usernames or password must not be disclosed
 - They immediately report any illegal, inappropriate or harmful material or incident, to a member of the Senior Leadership team.
 - Staff do not access, copy, remove or otherwise alter any other user’s files, without their express permission.
 - Staff communicate with others in a professional manner,
 - Ensure that staff gather / or publish images of others with their permission and in accordance with the school’s policy on the use of digital / video images.
 - Staff avoid opening any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
 - Staff avoid making large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
 - Staff do not install or attempt to install programmes of any type on a machine, or store programmes on a computer, try to alter computer settings, unless this is allowed in school policies.
 - Staff do not disable or cause any damage to school equipment, or the equipment belonging to others.
 - Staff understand that the data protection policy requires that any staff or young person’s data will be kept private and confidential, except when it is deemed necessary to disclose such information to an appropriate authority.
 - Staff immediately report any damage or faults involving equipment or software, however this may have happened.
 - Staff ensure that they have permission to use the original work of others in their own work

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.
- 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 must be professional in tone and content.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

School staff should ensure that:

- No reference should be made, in personal social media accounts, 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 committee to ensure compliance with the relevant policies.

Unsuitable / inappropriate 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 school or outside school when using school equipment or systems. The school policy restricts usage as follows:

		Unacceptable	Unacceptable and illegal
User Actions 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 (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	

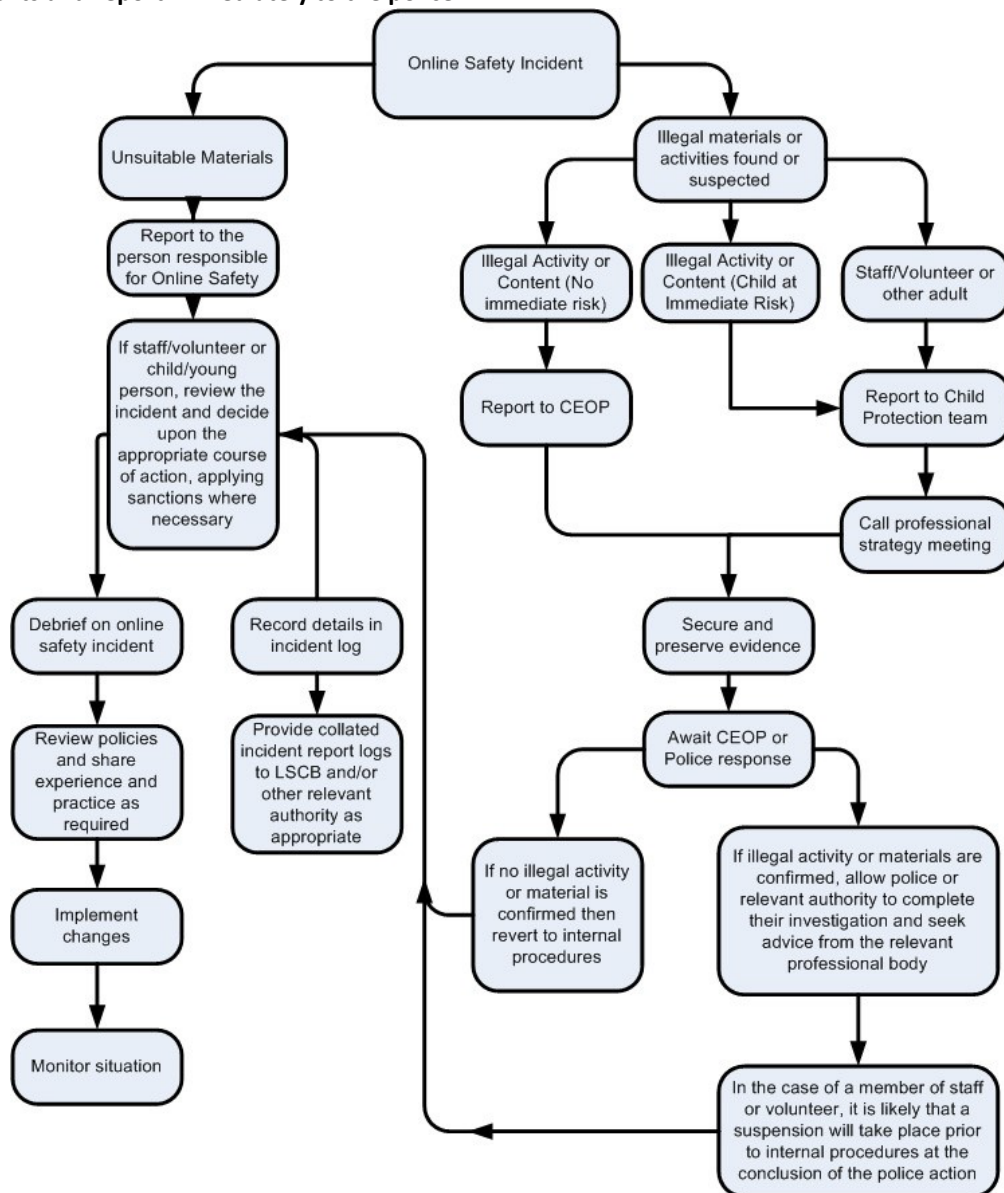
[DG(MS2)]

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

All members of the school community should be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority 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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

E safety Reporting Log

Signature									
Incident									
Action taken	By whom?								
	What?								
Incident									
Time									
Date									

E-Safety Group Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The e-safety group will seek to include representation from all stakeholders. The composition of the group should include SLT member/s

- Designated Safeguarding Officer /E-safety Officer
- Data protection officer
- Teaching staff
- Support staff
- Governor
- Parent
- ICT Technical Support staff
- *Pupil representation – for advice and feedback. Pupil voice is essential in the make up of the e-safety group, but pupils would only be expected to take part in committee meetings where deemed relevant.*

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3 members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. CHAIRPERSON

A suitable Chairperson should be selected from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. DURATION OF MEETINGS

Meetings shall be held termly for a period of 1 hour. A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the E-safety Officer with the following:

- To annually review and develop the e-safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the e-safety policy
- To monitor the log of reported e-safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-safety. This could be carried out through:
 - Staff meetings
 - Student / pupil forums (for advice and feedback)
 - Governors meetings

- Surveys/questionnaires for students / pupils, parents / carers and staff
- Parents evenings
- Website/Newsletters
- E-safety events
- Internet Safety Day (the second Tuesday in February)
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the school
- To monitor incidents involving cyberbullying for staff and pupils

6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for West Monmouth School have been agreed

Signed by (SLT):

Date:

Date for review:

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
 - Ascertain whether the communication is business or personal;
 - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1977

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The GDPR (General Data Protection Regulation) 2018

Replaced the current Data Protection Act (DPA) and is set to strengthen and unify all data held within an organisation. For schools, GDPR brings a new responsibility to inform parents and stakeholders about how they are using pupils’ data and who it is being used by.

- Under GDPR, consent must be explicitly given to anything that isn’t within the normal business of the school, especially if it involves a third party managing the data. Parents (or the pupil themselves depending on their age) must express consent for their child’s data to be used outside of the normal business of the school.
- Schools must appoint a Data Protection Officer and be able to prove that they are GDPR compliant.
- Schools must ensure that their third party suppliers who may process any of their data is GDPR compliant and must have legally binding contracts with any company that processes any personal data. These contracts must cover what data is being processed, who it is being processed by, who has access to it and how it is protected.
- It will be compulsory that all data breaches which are likely to have a detrimental effect on the data subject are reported to the ICO within 72 hours.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

Links to other organisations or documents

The following links may help when extra advice is required in relation to this policy.

UK Safer Internet Centre

[Safer Internet Centre -](#)

[South West Grid for Learning](#)

[Childnet](#)

[Professionals Online Safety Helpline](#)

[Internet Watch Foundation](#)

CEOP

<http://ceop.police.uk/>

[ThinkUKnow](#)

Others:

INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis

Netsmartz <http://www.netsmartz.org/index.aspx>

Support for Schools

Specialist help and support [SWGfL BOOST](#)

Cyberbullying

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government [Better relationships, better learning, better behaviour](#)

[DCSF - Cyberbullying guidance](#)

[DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies](#)

Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>

Cyberbullying.org - <http://www.cyberbullying.org/>

Social Networking

Digizen – [Social Networking](#)

[SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](#)

[Connectsafely Parents Guide to Facebook](#)

[Facebook Guide for Educators](#)

Curriculum

[SWGfL Digital Literacy & Citizenship curriculum](#)

Glow - <http://www.educationscotland.gov.uk/usingglowandict/>

Alberta, Canada - [digital citizenship policy development guide.pdf](#)

Teach Today – www.teachtoday.eu/

Insafe - [Education Resources](#)

Somerset - [e-Sense materials for schools](#)

Mobile Devices / BYOD

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)

NEN - [Guidance Note - BYOD](#)

Data Protection

Information Commissioners Office:

[Your rights to your information – Resources for Schools - ICO](#)

[ICO pages for young people](#)

[Guide to Data Protection Act - Information Commissioners Office](#)

[Guide to the Freedom of Information Act - Information Commissioners Office](#)

[ICO guidance on the Freedom of Information Model Publication Scheme](#)

[ICO Freedom of Information Model Publication Scheme Template for schools \(England\)](#)

[ICO - Guidance we gave to schools - September 2012 \(England\)](#)

[ICO Guidance on Bring Your Own Device](#)

[ICO Guidance on Cloud Hosted Services](#)

[Information Commissioners Office good practice note on taking photos in schools](#)

[ICO Guidance Data Protection Practical Guide to IT Security](#)

[ICO – Think Privacy Toolkit](#)

[ICO – Personal Information Online – Code of Practice](#)

[ICO – Access Aware Toolkit](#)

[ICO Subject Access Code of Practice](#)

[ICO – Guidance on Data Security Breach Management](#)

SWGfL - [Guidance for Schools on Cloud Hosted Services](#)

LGfL - [Data Handling Compliance Check List](#)

Somerset - [Flowchart on Storage of Personal Data](#)

NEN - [Guidance Note - Protecting School Data](#)

Professional Standards / Staff Training

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

Kent - [Safer Practice with Technology](#)

Childnet / TDA - [Social Networking - a guide for trainee teachers & NQTs](#)

Childnet / TDA - [Teachers and Technology - a checklist for trainee teachers & NQTs](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure / Technical Support

Somerset - [Questions for Technical Support](#)

NEN - [Guidance Note - esecurity](#)

Working with parents and carers

SWGfL / [Common Sense Media Digital Literacy & Citizenship Curriculum](#)

[SWGfL BOOST Presentations - parents presentation](#)

[Connect Safely - a Parents Guide to Facebook](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[DirectGov - Internet Safety for parents](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops / education](#)

[The Digital Universe of Your Children - animated videos for parents \(Insafe\)](#)

[Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](#)

[Insafe - A guide for parents - education and the new media](#)

[The Cybersmile Foundation \(cyberbullying\) - advice for parents](#)

Research

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)

[Futurelab - "Digital participation - its not chalk and talk any more!"](#)

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
DPO	Data protection officer
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System

NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

This document has been produced in line with SWGfL guidance and template policy.