WINMARLEIGH C.E. SCHOOL

Online Safeguarding Policy

October 2024

Development / Monitoring / Review of this Policy

This Online Safeguarding policy has been developed by a working group made up of:

- Headteacher
- Computing Subject Leader
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers

Schedule for Development / Monitoring / Review

This Online Safeguarding Policy was approved by the Governing Body on	01/10/24
The implementation of this Online Safeguarding Policy will be monitored by the:	DSL Computing Subject Leader On-Line Safety Champion (Chair of Governors)
Monitoring will take place at regular intervals:	Our system is filtered by Surf Protec (Ed-It) Fortnightly check on filtering email alerts sent to head / Subject Leader/Online Safety Champion (Chair of Governors).
The Governing Body will receive a report on the implementation of the Online Safeguarding Policy generated (which will include anonymous details of online safety incidents) at regular intervals:	Termly
The Online Safeguarding Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Reviewed – Autumn Term 2024-25
Should serious online safety incidents take place, the following external persons / agencies may be informed:	LA Safeguarding Officer Governing Body LADO Police

The school will monitor the impact of the policy using:

- Logs of reported incidents via CPOMS
- Monitoring logs of internet activity (including sites visited) / filtering
- Surveys / questionnaires of
    - students / pupils (annually)
    - staff

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 Online Safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school, including use of or membership of social networking sites which have age restrictions.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the Online Safeguarding Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Champion. The role of the Online Safety Champion will include:

- regular meetings with the Computing Subject Leader
- regular monitoring of online safety incident logs on CPOMS
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting

Headteacher (DSL) and Senior Leaders:

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for monitoring online safety will be delegated to the Computing Subject Leader, but responsibility for challenging misuse still falls with the Headteacher as the designated senior leader for child protection.

- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR disciplinary procedures).

• The Headteacher and Senior Leaders are responsible for ensuring that the Computing Subject Leader receives suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

• The Headteacher and governing body and Subject Leader will receive regular monitoring reports from the filter and any incident reports.

• Liaises with EdIT to administer filtering software and report generating, reviewing filtering log reports on a fortnightly basis

Computing Subject Leader: Mrs S. Shaw

• works in partnership with the DSL (Headteacher)

• takes day to day responsibility for reporting online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents

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

• provides training and advice for staff

• liaises with the Local Authority / relevant body

• liaises with school technical staff

• receives reports of online safety incidents and has access to DSL CPOMS network with alert setting for online safeguarding and cyber bullying.

• reports to the Online Safety Champion (Mrs L Sutcliffe) to discuss current issues, review incident logs and filtering / change control logs.

• attends relevant Governors meetings

• reports regularly to Senior Leadership Team

Technical staff (Ed-It Solutions Ltd):

The Technical Staff are responsible for ensuring:

• that the school's technical infrastructure is secure and is not open to misuse or malicious attack.

• that the school meets required online safety technical requirements and any Local Authority Online Safeguarding Policy/ Guidance that may apply.

• that users may only access the networks and devices through a properly enforced password protection policy. Staff users will be responsible for maintaining the security of their own passwords. KS2 users will have their own passwords (generated for them). KS1 users will have a class log in which is monitored by class staff when being used.

• the filtering procedure is applied and updated on a regular basis

• that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- that the use of the network / internet / Learning Platform / remote access / email can be monitored if any suspected misuse / attempted misuse is reported to the Headteacher or Computing Subject Leader for investigation / action / sanction

- that monitoring software / systems are implemented and updated as agreed in school

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safeguarding Policy and practices

- as part of the induction pack, have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)

- they report any suspected misuse or problem to the Headteacher or Computing Subject Leader for investigation / action / sanction via CPOMs

- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems

- online safety issues are embedded in all aspects of the curriculum and other activities

- pupils understand and follow the Online Safeguarding Policy and acceptable use policies

- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- in lessons where internet use is pre-planned 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.

- Information on websites the children will be asked to access in their work or on any individual(s) (e.g. digital expert/mystery skype) the children will be interacting with online will be shared with parents in advance.

- Teachers will inform parents of which staff will be interacting with their children online (through Seesaw) at the beginning of each academic year.

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data

- access to illegal / inappropriate materials

- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

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 online safety practice when using digital technologies out of school and realise that the school's Online Safeguarding 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 online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- supporting the school in the ban on their children bringing personal devices into school without prior permission
- supporting the appropriate use of 'personal data' by refraining from sharing any pictures taken of their child during school events (or from Seesaw) that include other children in any way.

Community Users

Only school staff (including supply where appropriate) will be allowed access to school networks. Any outside or community visitors that want to use digital resources (e.g. PPT) will be required to email resources to the bursar or class teacher concerned before their visit.

Policy Statements

Education –Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities.

A planned online safety curriculum is provided through use of the "Project Evolve" digital literacy resources but should also be a part of Computing / PSHE / other lessons and should be regularly revisited.

- Key online safety messages should be reinforced as part of a planned programme of assemblies and 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 be critically aware of the exploitative interests of others online such as advertising, phishing and scams and other exploitative commerce activities.

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

- Staff should act as good role models in their use of digital technologies the internet and mobile devices

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

- Where pupils are allowed to freely search the internet (in a pre-planned context), staff should be vigilant in monitoring the content of the websites the children visit

- It is accepted that from time to time, for good educational reasons, children 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 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. Requests should also include the time period for which the exemption should be required.

- Pupils will be taught how to report any unpleasant internet content

- Pupils will be shown how to publish and present information to a wider audience.

Publishing pupils' images and work

• Pupils' full names will not be used anywhere on any online space, particularly in association with photographs

• Written permission from parents/carers will be obtained before photographs are published on the school website

• Work will only be published with the permission of the pupil and parents/carers

• Parents will be clearly informed of the school policy on image taking and publishing

Social networking and personal publishing

• The school will control access to social networking sites, and consider how to educate pupils in their safe use (e.g. Seesaw for in class/homework work)

• Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location

• Pupils and parents will be advised that the use of social network spaces outside school bring a range of dangers for primary aged pupils

• Where pupils discuss content on social media pages, where there is an age limit on these sites, and there is any reason to believe a child may be accessing these sites, parents will be informed at the earliest opportunity so that they can monitor their child's on-line habits (for example, Facebook has a minimum age requirement of 13 years)

Education – Parents / Carers

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

• Curriculum activities

• Specialist visits (safeguarding consultant meetings/briefings from Lancs)

• Letters, newsletters, web site,

• High profile events / campaigns e.g. Safer Internet Day

• Through other focus weeks eg, Anti Bullying week

• Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

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

- The school website will provide online safety information for the wider community

Education & Training – Staff / Volunteers

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

- All new staff and volunteers should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safeguarding Policy and Acceptable Use Agreements

- It is expected that some staff will identify online safety as a training need within the appraisal process

- The Computing Subject Leader will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations

- This Online Safeguarding Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days

- The Computing Subject Leader will provide advice / guidance / training to individuals as required.

Training – Governors

Governors awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL)

- Participation in school training (this may include attendance at assemblies / lessons)

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

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

• Servers, wireless systems and cabling must be securely located and physical access restricted

• All users will have clearly defined access rights to school technical systems and devices

• All users (at KS2 and above and including any supply staff) will be provided with individual username and secure password by the school (Computing lead / Ed-It Solutions Ltd), who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.

• KS1 users will have a class login into the network. Usage will be closely monitored by staff.

• The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (school safe)

• The Computing Subject Leader / Technical assistance (ED IT SOLUTIONS) 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)

• Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored by Ed-It Solutions and any breaches are reported to the headteacher. There is a clear process in place to deal with requests for filtering changes (see appendix for more details)

• Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet

• The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for staff / pupils)

• 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 procedure is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems via account with appropriate level of filtering

• An agreed policy is in procedure regarding the extent of personal use that users (staff / students) and their family members are allowed on school devices that may be used out of school

• An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by external users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage. Devices owned by staff (and children) may also have access to 'data' based internet and therefore be unlimited and unrestricted in their access. Such devices are unsuitable for this environment and should not be used in lessons or be brought in by children (see below table).

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy is consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies

- The school allows:

	School Devices		Personal Devices		
	School owned for single user	School owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	No	Yes But not in the presence of children	Yes But not in the presence of children
Full network access	Yes	Yes	No	No	No
Internet only	Yes	Yes	No	No	No without prior permission
To be restricted from network access	No	No	n/a	Yes	Yes

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press (Seesaw/school home-school learning app is an exception to this as it is a closed password protected area).

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute

- Pupils must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs

- Pupil's work can only be published with the permission of the pupil and parents or carers (Seesaw/school home-school learning app is an exception to this as it is a closed password protected area).

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				Students/Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	**X**							**X**
Use of mobile phones in lessons				**X**				**X**
Use of mobile phones in social time		**X**						**X**
Taking photos on mobile phones/cameras				**X**				**X**
Use of other mobile devices e.g tablets, gaming devices		**X**					**X**	
Use of personal email addresses in school, or on school network		**X**						**X**
Use of school email for personal emails	**X**						**X**	
Use of messaging apps		**X**						**X**
Use of social media		**X**						**X**
Use of blogs		**X**					**X**	

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 can be monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)

- Users must immediately report, through CPOMS and to the nominated person – in accordance with the school safeguarding policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications

- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details and commerce/phishing hazards. 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, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published

- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues

- Clear reporting guidance, including responsibilities, procedures and sanctions

- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers, school staff or school business.

- 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

- It is considered inappropriate for any staff member to be 'friends' with or 'connected' to parents or children within the school community via any social media. These connections are strongly advised against by the school. Any breaches of the above protocol caused by continued social media connections could result in disciplinary action.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school

- The school should effectively respond to social media comments made by others according to a defined policy or process, after seeking advice from the LA

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. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated/staff users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that 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**	

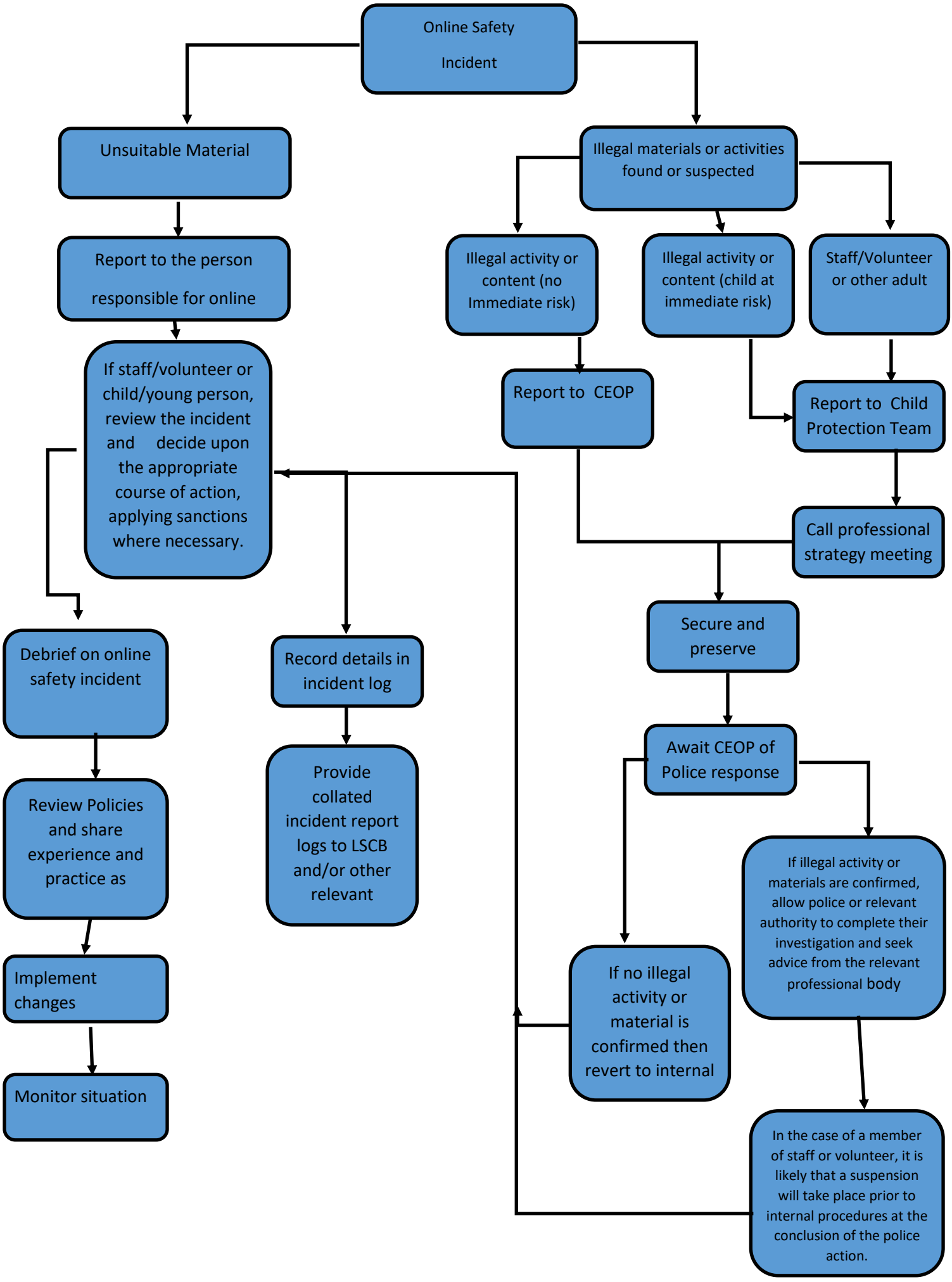
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems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

Responding to incidents of misuse

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

Illegal Incidents

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


Online Safety Incident
Unsuitable Material
Illegal materials or activities found or suspected
Report to the person responsible for online
Illegal activity or content (no Immediate risk)
Illegal activity or content (child at immediate risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary.
Report to CEOP
Report to Child Protection Team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve
Review Policies and share experience and practice as
Provide collated incident report logs to LSCB and/or other relevant
Await CEOP of Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action.

Other Incidents

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

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 attached to CPOMS entries or oriented, signed and attached to the DSL's own records (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
- promotion of terrorism or extremism
- 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 & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Actions / Sanctions **Students / Pupils Incidents**	Refer to class teacher	Refer to Computing Subject Lead for action re filtering / security etc.	Warning	Refer to Headteacher	Inform parents / carers	Refer to Police detention
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	**X**	**X**	**X**	**X**	**X**	**X**
Unauthorised use of non-educational sites during lessons	**X**	**X**	**X**			
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	**X**		**X**		**X**	
Unauthorised / inappropriate 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**	
Attempting to access or accessing the school network, using another student's / pupil's account	**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**	
Corrupting or destroying the data of other users	**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**	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		**X**	**X**	**X**	**X**	
Using proxy sites or other means to subvert the school's / academy's filtering system	**X**	**X**	**X**	**X**	**X**	
Accidentally accessing offensive or pornographic material and failing to report the incident	**X**	**X**	**X**			
Deliberately accessing or trying to access offensive or pornographic material	**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**	

Staff Incidents	Refer to Technical Support Staff for action re filtering	Refer to Headteacher	Warning	Suspension Refer to Local Authority /HR/LADO	Refer to Police
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X		X	X
Inappropriate personal use of the internet / social media / personal email	X	X	X		
Unauthorised downloading or uploading of files		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		
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	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X	X	X
Actions which could compromise the staff member's professional standing		X	X	X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X	X	X	
Using proxy sites or other means to subvert the school's filtering system	X	X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	
Breaching copyright or licensing regulations		X	X		
Continued infringements of the above, following previous warnings or sanctions		X	X	X	

Appendix

Acknowledgements

We would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy:

- Members of the SWGfL Online Safety Group
- The Police
- Representatives of Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

UK Safer Internet Centre

Safer Internet Centre - http://saferinternet.org.uk/

South West Grid for Learning - http://swgfl.org.uk/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

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/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

Bullying / Cyberbullying

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/

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

Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) - http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcomingcyberbullying-work

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

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

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/

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

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

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 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

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 Digital Literacy & Citizenship curriculum

Online Safety BOOST Presentations - parent's presentation

Connectsafely Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

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!"

Ofcom – Children & Parents – media use and attitudes report – 2015

Legislation

Schools should be aware of the legislative framework under which this Online Safeguarding Policy template and guidance 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.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

• Fairly and lawfully processed.

• Processed for limited purposes.

• Adequate, relevant and not excessive.

• Accurate.

• Not kept longer than necessary.

• Processed in accordance with the data subject's rights.

• Secure.

• Not transferred to other countries without adequate protection.

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.

Appendices

Pupil Acceptable Use Agreement – for Key Stage 2 pupils

School Policy Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

• that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.

• that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

ENJOY BELIEVE ACHIEVE

Key Stage 2 Rules for Responsible ICT Use

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my login and password secret.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and I will only access websites that are relevant to my learning.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission from a teacher.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult immediately.

Key Stage 2 E-safety Agreement Form 2024-25

Pupil name: _____

I have read the school 'rules for responsible ICT use'. ☐

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules. ☐

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way. ☐

I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, that they may contact my parent / carer. ☐

Pupil's signature _____

Parent / Guardian signature _____

Date: ___/___/___

Please return this form to school.

ENJOY BELIEVE ACHIEVE

Foundation Stage and Key Stage 1 ICT Pupil Rules 2024-25

1. I will always ask the teacher before I use the Internet and will be sensible whenever I use it.
2. I will only use the computers for schoolwork and will only use websites my teacher has told me about.
3. I will not give my name, address or telephone number to anyone on the Internet.
4. I will NEVER agree to meet someone I have spoken to on the Internet.

(Please return the slip below when your child has signed it)

Foundation Stage and Key Stage 1

E-safety Agreement Form

Pupil name: _____

My parents / teacher have explained the ICT rules to me.

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

Pupil's signature _____

Date: ___/___/___

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

PARENTAL CONSENT FORM – PHOTOGRAPHS/IMAGES

Name of Child: _____

Photographs

Frequently, we take photographs of the children at our school. These images may be used in our school prospectus, in other printed publications that we produce, on our school website, or on project display boards in school. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use.

Occasionally, our school may be visited by the media who will take photographs or film footage of a high profile event, or to celebrate a particular achievement. Pupils will often appear in these images, which may appear in local or national newspapers or on television news programmes. **(See attached sheet for Conditions of Use for more information on use of images by the media).**

In order that we can protect your child's interests, and to comply with GDPR, **please read the Conditions of Use attached to this form before answering questions 1-5 below and signing and dating this form. Please return completed form (one for each child) to school as soon as possible.**

(Please tick)

1. May we use your child's photograph in the school prospectus and other printed publications that we produce for promotional purposes, or on project display boards, etc.? ☐ Yes ☐ No

2. May we use your child's image on our school website? ☐ Yes ☐ No

3. May we record your child's image on video? ☐ Yes ☐ No

4. May we allow your child to appear in the media as part of school's involvement in an event? This could include being on their website. ☐ Yes ☐ No

5. May we use your child's image on our closed Winmarleigh school Facebook page or the closed Winmarleigh community Facebook page? ☐ Yes ☐ No

6. I will not share any image which contain images of other children in school on any social media site ☐

(Please note Conditions of Use attached to this form).

I have read and understood the conditions of use attached to this form.

Parent's or Carer's Signature: _____

Name (block capitals please): _____

Date: _____

CONDITIONS OF USE

1. This form is valid for the period of time your child attends this school and your child's image will not be used for any new publicity after this time. Any existing publicity materials may, however, may continue to be used for up to 3 years after your child leaves. Your consent will automatically expire after this time.

2. The school will not use the personal details or full names (which means first name **and** surname) of any child or adult in a photographic image, on video, on our website, in the school prospectus or in any of our other printed publications.

3. The school will not include personal e-mail or postal addresses or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.

4. If we use photographs of individual pupils, we will not use the full name of that child in any accompanying text or caption.

5. If we use the full name of a pupil in the text, we will not use a photograph of that child to accompany the article.

6. We may include pictures of pupils and teachers that have been drawn by pupils. We may use groups or class photographs or footage with very general labels, such as "a science lesson".

7. We will only use images of pupils who are suitably dressed.

8. We may post pictures on our 'closed' Facebook page or the Winmarleigh Community 'closed' Facebook page. Only people with permission can access these pages.

9. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

Notes on Use of Images by the Media

If you give permission for your child's image to be used by the media then you should be aware that:

- The media will want to use any printed or broadcast media pictures that they take alongside the relevant story;
- It is likely that they will wish to publish the child's name, age and the school name in the caption for the picture (possible exceptions to this are large group or team photographs);

It is possible that the newspaper will re-publish the story on their website, or distribute it more widely to other newspapers or media organisations.

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

ENJOY BELIEVE ACHIEVE

Staff (and Volunteer) Acceptable Use Policy Agreement 2024-25

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published publically (eg on the school website or whole class VLE posts) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.

- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use.

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: …….

Signed: …….

Date: ……..

Glossary of Terms

AUP / AUA	-	Acceptable Use Policy / Agreement – 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.
CPD	-	Continuous Professional Development
FOSI	-	Family Online Safety Institute
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 online safety programmes for schools, young people and parents
VLE	-	Virtual Learning Environment (a software system designed tto support teaching and learning in an educational setting,
WAP	-	Wireless Application Protocol
UKSIC	-	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

Copyright of the SWGfL School Online Safeguarding Policy Templates is held by SWGfL. Schools any other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.