NURTURE – EMPOWER - ACHIEVE

Gilwern Primary School

Online Safety Policy

Nurture, Empower, Achieve
The School's Vision

- Gilwern School creates a happy, secure and stimulating environment, where learners are encouraged to reach their full potential.
- The school works collaboratively with others to develop ambition, enterprise, ethics and health in our learners, by providing exciting, authentic, learning experiences.
- All staff are committed to develop learners' English and Welsh literacy, numeracy and digital competence skills through a meaningful broad and balanced curriculum to enhance their life chances.

The School's Aims

- To create a nurturing environment where children, staff and other stakeholders develop positive values and attitudes, in order to become responsible global citizens.
- To inspire and enthuse individuals to work creatively with both independence and collaboration to reach their goals.
- To identify and build upon individuals' strengths, enabling learners to confidently apply their knowledge and skills in an ever-changing world.

The School's Strategic Objectives

- As a school we cater for all and are not discriminatory. Equity is provided to ensure all learners have equal access to the vision of school.
- Develop links with organisations who support learners, to ensure the school's wider contribution to the community is valued.
- Through the process of self-evaluation identify strengths and areas for development to ensure continuous improvement and implementation of national priorities.
- Recruit and retain quality staff who are committed to continuous professional development and are able to deliver inspirational and innovative learning experiences.
- Leadership provides a clear, shared vision where success is achieved through mutual cooperation, empowerment and ownership.
- The school provides a rich understanding of Wales locally, nationally and in an international context.

We are a Rights Respecting School

In 1991 our Government signed up to the United Nations Convention on the Rights of the Child (UNCRC). In signing the Convention, the 54 articles laid down have become enshrined in UK law. The Convention applies to everyone.

At Gilwern Primary School we aim to work within the spirit as well as the letter of the Convention and our school policies and home-school agreement is based around these rights and responsibilities. At Gilwern Primary School we work together so that the rights of the child are ensured and their responsibilities are clear.

The process of raising safeguarding and Child Protection concerns in relation to Prevent is the same as for all safeguarding concerns. The school will contact Children's Services and will discuss the concerns with the Duty Officer, and a multi- agency referral form (MARF) is completed and submitted to Children's Services via childduty@monmmouthshire.gcsx.gov.uk . Once assessed by the FST (duty team) manager and Prevent SPOC in the local authority, a decision will be made as to whether a Channel Referral is required. If a Channel referral is required, the Prevent SPOC will assist the school in completing the referral form and the school will participate on the Channel Panel."

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.

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of: *Headteacher/ Safeguarding officer*

- *Senior Leadership Team*
- *ICT Coordinator*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*
- *Parents and Carers*
- *Community users*

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

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

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 Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing body / Governor's sub-committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body should take on the role of Online Safety Governor to include:

- regular meetings with the Online Safety Co-ordinator / Safeguarding Officer
- regular monitoring of Online Safety incident logs
- reporting to Link Governor

Headteacher and Senior Leaders:

- The Headteacher and Senior Leaders have a duty of care for ensuring the safety (including Online Safety) of members of the school community. The day to day responsibility for Online Safety is that of the Online Safety Coordinator, who will ensure open communication with the Safeguarding Officer.
- 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 Online Safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Coordinator / Safeguarding Officer and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive half termly monitoring reports from the Online Safety Co-ordinator / Safeguarding Officer following meeting with Link Governor and pupil representatives.

Safeguarding Officer:

The Safeguarding Officer

- is trained in Online Safety issues and is aware of the potential for serious safeguarding issues to arise from:
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Liaises with the Local Authority / relevant body
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- meets half termly with Online Safety Governor to discuss current issues, review incident logs and if possible, filtering / change control logs
- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Online Safety Coordinator

The Online Safety Coordinator

- leads the Online Safety committee
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- provides (or identifies sources of) training and advice for staff
- liaises with (school) technical staff
- meets half termly with Online Safety Governor to discuss current issues, review incident logs and if possible, filtering / change control logs
- reports half termly to Senior Leadership Team

Network Manager / Technical staff (SRS):

Managed Service Provider is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets (as a minimum) the required Online Safety technical requirements as identified by the Local Authority and also the Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that the filtering policy (if one exists), is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy Template" for good practice)
- 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 / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher/Senior Leadership Team; e-Safety Coordinator / Safeguarding Officer/Link governor for investigation / action
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher /Senior Leadership Team ; Online Safety Coordinator / Safeguarding Officer for investigation / action
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems (Hwb, Class Dojos)
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety and acceptable use agreements / 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

Online Safety Group

The School Online Safety & Digital Leader Group undertakes the role of monitoring Online Safety. They are a consultative group that has wide representation from the school community, and discuss issues regarding Online Safety and monitoring the Online Safety policy including the impact of initiatives.

Members of the School Council will assist the Online Safety Coordinator with:

- Review and monitoring of the school Online Safety policy / documents.
- consulting stakeholders – including parents / carers and the students / pupils about the Online Safety provision
- promote online safety throughout the school
-

Learners

- 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 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 / VLE 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
- access to parents' sections of the website / VLE and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)
- online safety awareness delivered by Online Safety Coordinator annually.
- Reference to the relevant web sites / publications eg https://hwb.wales.gov.uk/ www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Community Users

Community Users who access school systems / website / VLE as part of the wider school provision will be made aware of Online Safety Procedures before being provided with access to school systems.

Policy Statements

Distance & Blended Learning
All learners, staff, parents and carers will conduct themselves safely and adhere to the User Agreement whilst facilitating and undertaking learning through digital portals. Teaching staff will continue to reinforce key online safety messages throughout any distance/blended learning periods. Please see Distance and Blended Learning Policy for details around pedagogy and practice.

Learners

Online Safety is a part of all areas of the curriculum and staff reinforce Online Safety messages through values-based education. The Online Safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned Online Safety curriculum is provided as part of Health and Wellbeing Area of Learning Experience
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and homelearning activities
- Learners are taught to be critically aware of the materials / content they access on-line and guided to validate the accuracy of information.
- Learners are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Leaners are 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 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 learners are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, learners 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.

Technical – infrastructure / equipment, filtering and monitoring

The schools managed ICT service provider is responsible for carrying out all the Online Safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school Online Safety Policy / Acceptable Use Agreements. In addition, the school checks their Local Authority / other relevant body policies on these technical issues if the service is not provided by the Authority.

Schools Resource Service (SRS) are 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;

- 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 the ICT curriculum team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- 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.
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

<u>Use of BYOD must not introduce vulnerabilities into existing secure environments.</u>

A device may be a privately owned smartphone, tablet, notebook / laptop, camera or other new technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet including the school's (Hwb+) learning platform and other cloud-based services such as email and data storage. The device may typically also be used for the taking of images, for the recording of sounds or video and for generating and storing a wide range of other types of data (often as a result of using an app).

Critical BYOD is that the staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device they use is user or school owned. This understanding then underpins further conventions around acceptable use of both the devices and of the wider network.
The essential principle of safe and responsible use of the internet and learning technologies sits with the understanding that this technology is allowed primarily for educational purposes.

Use of digital and video images

Staff, parents / carers and students / pupils are aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate learners 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.
- 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. At the beginning of each academic year the school will communicate the policy regarding acceptable use of videos and digital images to parents/carers.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Learners must be monitored by class teacher or a responsible adult when taking and sharing digital images.
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs/video of learners are published on the school website following Monmouthshire County Council policy.
- Parents will need to sign an agreement that their use of digital or video images will abide by the 'Acceptable Use' guidelines.

Data Protection

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

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

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a procedure for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear procedures about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete
- All portable data storage devices are to be encrypted by the Schools Resource Service (SRS)

Communications

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

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and learners should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report to the nominated person – in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and learners or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Whole class / group email addresses may be used at Foundation Phase, while learners at Key Stage 2 and above will be provided with individual school email addresses for **educational use.**
- Learners are 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 will not be posted on the school website and only official email addresses will be used to identify members of staff.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Expectations for teachers' and teaching support staffs' professional conduct are set out by the Education Workforce Council Wales (EWC) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

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. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for learners and their families and for colleagues and the learning setting.

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

<u>All School staff should ensure that:</u>

- They do not engage in online discussion on personal matters relating to members of the school community
- Security settings on personal social media profiles are regularly checked by the individual to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior Safe Guarding officer and Online Safety coordinator committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

<u>Unsuitable / inappropriate activities</u>

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg 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 school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain	Acceptable for nominated	Unaccepta	Unaccepta ble and
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	
On-line gaming (educational)				X		
On-line gaming (non educational)					X	

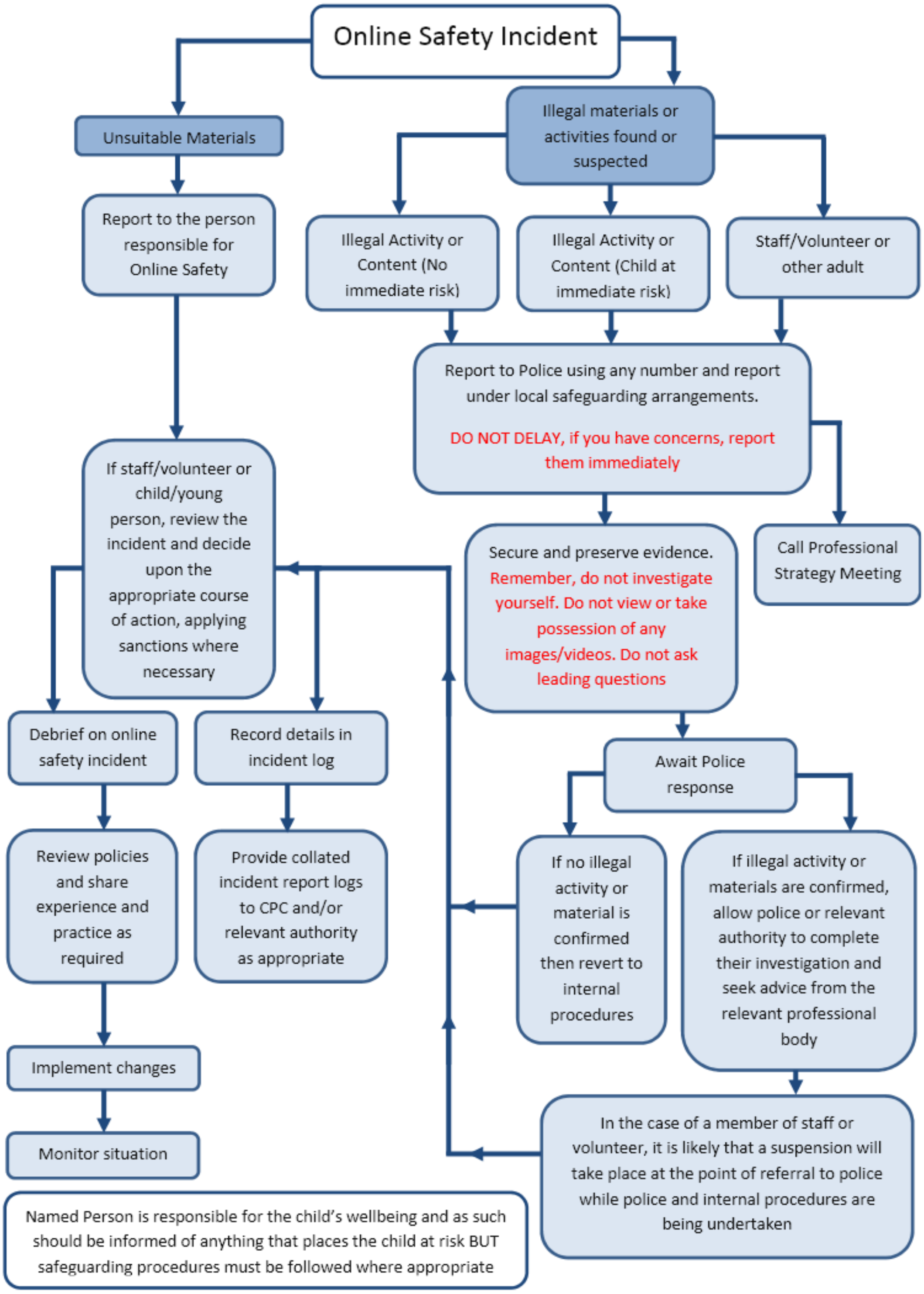
On-line gambling			X	
On-line shopping / commerce		X		
File sharing		X		
Use of social media			X	
Use of messaging apps		X		
Use of video broadcasting eg Youtube		X		

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. All of these incidents must be reported to the Safeguarding Officer who will then enter them onto an incident log. **(Safeguarding Log held in class records/with safeguarding officer)**


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

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 printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School Actions

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

Students / Pupils **Actions**

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

Staff **Actions**

Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				X
Inappropriate personal use of the internet / social media / personal email	X	X	X					
Unauthorised downloading or uploading of files	X	X	X		X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X	X		X			
Careless use of personal data eg holding or transferring data in an insecure manner	X	X	X		X			
Deliberate actions to breach data protection or network security rules	X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X				
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing	X	X	X			X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X	X		X	X	X
Using proxy sites or other means to subvert the school's 's filtering system	X	X	X	X	X			
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X	X	X				

Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

Acknowledgements

Gilwern's Online Safety Policy was developed with the support of the e-Safety Policy Template available at http://hwb.wales.gov.uk/Resources/resource/de0f0869-7cb9-4688-bce2-8b1945e905e7
WG and SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of the School e-Safety Policy Template and of the 360 degree safe e-Safety Self Review Tool:

- Members of the SWGfL e-Safety Group
- Representatives of SW Local Authorities
- Representatives from a range of Welsh schools involved in consultation and pilot groups
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in October 2014. However, SWGfL cannot guarantee it's accuracy, nor can it accept liability in respect of the use of the material.

NURTURE EMPOWER ACHIEVE

Gilwern Primary School

Appendices

Appendix 1 – Staff Acceptable Use Policy Agreement

Appendix 2 – Pupil Acceptable Use Policy Agreement (Foundation Phase – Year 3)

Appendix 3 – Parents/Carers Digital Agreement

Appendix 4 – School Technical Security Policy

Appendix 5 – Summary of Legislation

Appendix 6 – Glossary of Terms

NURTURE EMPOWER ACHIEVE

Gilwern Primary School

Staff Acceptable Use Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools 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 internet access 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 ICT 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 ICT in their everyday work.

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg 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 ICT 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. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- 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 (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- 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 (PDAs / laptops / 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 ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. (schools / academies should amend this section in the light of their policies on installing programmes / altering settings)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital

personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or student / 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 Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT 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 (schools should amend this section to provide relevant sanctions as per their behaviour policies) 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 ICT 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

NURTURE EMPOWER ACHIEVE

Gilwern Primary School

Pupil Acceptable Use Policy Agreement – for younger pupils (Foundation Phase – Year 3)

This is how we stay safe when we use computers:

I will ask a teacher or another adult from the school if I want to use the computers

I will only use activities that a teacher or another adult from the school has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or another adult from the school if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or another adult from the school if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

I would like my work to be displayed and shared on our school website and Purple Mash Display Board.

Signed (child):…………………………………………….

Signed (parent): …………………………………………..

NURTURE EMPOWER ACHIEVE

Gilwern Primary School

Pupil Acceptable Use Agreement (AUA) – for older pupils

(KS2 Year 4-6)

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 users at risk.**

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the **pupils to agree to be responsible users.**

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will **monitor** my use of IT systems, devices and digital communications.
- **I will keep my username and password safe and secure** – I will not share it, 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 be aware of **"stranger danger",** when I am communicating on-line.
- **I will not disclose or share personal information** about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a **public place** and **take an adult with me**.
- I will **immediately report** any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the **school systems and devices** are primarily intended for **educational use** and that I will not use them for personal or recreational use unless I have permission.
- **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 use** the school systems or devices for **on-line gaming**, **on-line gambling**, **internet shopping, file sharing**, or **video broadcasting** (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- **I will respect others'** work and property and **will not access**, **copy, remove** or otherwise **alter** any other user's **files**, without the owner's knowledge and permission.
- **I will be polite and responsible when I communicate with others,** I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- **I will not take or distribute images of anyone without their permission.**

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- **I will only use my own personal device(s) in school if I have permission.** I understand that, if I do use my own device(s) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- **I understand the risks and will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report** any damage or faults involving equipment or software, however this may have happened.
- **I will not open any hyperlinks** in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, 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 not install or attempt to install or store programmes of any type** on any school device, nor will I try to alter computer settings.
- **I will not use social media sites within school or using any school devices.**

When using the internet for research or recreation, I recognise that:

- I should ensure that **I have permission** to use the original work of others in my own work (Copyright)
- Where work is **protected by copyright,** I **will not** try to download copies (including music and videos)
- When I am using the internet to find information, **I should take care to check that the information** that I access **is accurate**, **as I understand** that **the work** of others **may not be truthful** and may be a deliberate attempt to mislead me.

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

- **I understand that the school also has the right to take action against me if it is brought to their attention that I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).**
- **I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action.** This may include loss of access to the school network / internet, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the following page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. <u>If you do not sign and return this agreement, access will not be granted to school systems and devices.</u>

NURTURE EMPOWER ACHIEVE

Student / Pupil Acceptable Use Agreement Form (KS2 Year4 -6)

This form relates to the Pupil Acceptable Use Agreement, to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) eg mobile phones, gaming devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this *school* eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil	
Class	
Signed	
Date	

Parent / Carer Countersignature

Signed	
Date	

NURTURE – EMPOWER - ACHIEVE

Dear Parent/Carer,

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They 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 Policy is intended to ensure:

- that young people 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 parents and carers are aware of the importance of e-Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement is attached to this permission form, so that parents / carers are aware of the school expectations of the young people in their care. This has been discussed with your child/children.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers ame Student / Pupil Name

As the parent / carer of the above child I give permission for my son / daughter to have access to the internet and to ICT systems and hardware at school.

Either: (KS2 and above)
I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (Foundation Phase and Year 3)
I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, e-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including applying monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Signed

Date

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / 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 can not 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 everyones 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.

Digital / Video Images Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *student / pupil*, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

Yes / No

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes / No

Signed

Date

School Technical Security Policy

Introduction

Please Note: Gilwern primary School will follow guidelines and procedures as provided by the Shared Resource Services (SRS)

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will monitor that SRS is maintaining responsibility for ensuring that the school infrastructure / network/ is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

The school has an externally managed ICT service. It is the responsibility of the school to ensure that SRS carry out all the e-Safety measures that might otherwise be carried out by the school itself (as suggested below). It is also important that the managed service provider is fully aware of the school e-Safety Policy / Acceptable Use Agreements. The school should also check their Local Authority / other relevant body policies / guidance on these technical issues if the managed service is not provided by the Authority.

Responsibilities

Technical Security

Policy statements

- 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
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (this may be at school, Local Authority or Managed Provider level).
- All users will have clearly defined access rights to school technical systems.

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- **Schools Resource Service** 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
- Mobile device security and management procedures are in
- School / Local Authority / Managed Service Provider 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. (
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential technical incident to the Online Safety Coordinator / Network Manager / Technician (or other relevant person, as agreed).
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) 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 users on school devices.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements:

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the e-Safety Committee (or other group).
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place eg school safe. Consideration should also be given to using two factor authentication for such accounts
- Passwords for new users, and replacement passwords for existing users will be allocated by. Any changes carried out must be notified to the manager of the password security policy (above).
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below.
- Requests for password changes should be authenticated by SRS to ensure that the new password can only be passed to the genuine user.

Staff passwords:

- All staff users will be provided with a username and password by SRS who will keep an up to date record of users and their usernames.
- for best practice, the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- for best practice, the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- for best practice, should be changed at least every 6 months, should not re-used for 6 months and be significantly different from previous passwords created by the same user - the last four passwords cannot be re-used .
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of school

Student / pupil passwords:

- All users will be provided with a username and password by SRS who will keep an up to date record of users and their usernames.
- Users will be required to change their password every academic year – unless breach of security occurs
- Students / pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness:

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-Safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in half termly online safety lessons

- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review:

SRS will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy

Summary of Legislation

Schools should be aware of the legislative framework under which this e-Safety 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.

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, grossly offensive, or threatening letter, electronic communication or other article to another person. It is also an offence to send information which is false and known or believed to be false by the sender.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Where the system controller has given express consent 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.

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).

Criminal Justice & Public Order Act 1994 / Public Order Act 1986

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 / Public Order Act 1986

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 Harrassment Act 1997

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.. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence is liable to imprisonment for a term of not more than 10 years, or to a fine or to both.

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.

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
- The right not to be subjected to inhuman or degrading treatment or punishment

The school is obliged to respect these rights and freedoms, but should balance 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 Protection of Freedoms Act 2012

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

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.
- CPD Continuous Professional Development
- CYPS Children and Young Peoples Services (in Local Authorities)
- FOSI Family Online Safety Institute
- EA Education Authority
- 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
-
- Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in October 2014. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

Further Guidance:

Schools may wish to seek further guidance. The following is recommended:

- NEN Technical guidance: http://www.nen.gov.uk/advice/266/nen-guidance-notes.html
- Somerset Guidance for schools – this checklist is particularly useful where a school uses external providers for its technical support / security:

http://www.360safe.org.uk/Files/Documents/Questions-for-Technical-Support-Somerset.aspx