

---

# ICT and E-Safety Policy

## Llangan Primary School

---



### Agreed Pupil Vision for ICT

Llangan Primary School has a vision for ICT and this is shared with all stakeholders. The vision informs the school development plan and directly impacts teaching and learning.

**“ICT is there to help us learn in all areas of school life and beyond. We learn to communicate safely and are prepared for the ever changing world ahead of us.”**

---

## UNCRC

The United Nations Convention on the Rights of the Child (UNCRC) is at the heart of our school's planning, policies, practice and ethos. As a Rights-Respecting School we not only teach about pupils's rights but also model rights and respect in all relationships. Our belief in "restorative approaches" ensures that every child is listened to.

## School perspective.

We strive to enable learners of all abilities to take greater control of their learning through the application of ICT in and out of school. This will be supported by the use of ICT in an effective way throughout the curriculum. Learners will develop the skills to know when it is most helpful to use ICT, and have the ability to use it efficiently when needed. As a school our aim is that learners achieve their full potential in their application of ICT throughout the curriculum.

We try to ensure that the continuing professional development of school staff and school leaders enables them to reach nationally defined standards of competence in ICT. School staff will endeavour to apply these competencies to improve the quality of teaching and learning. School leaders will apply these competencies to improve the quality of leadership and management.

As a school we provide support and opportunities for the use of ICT by ensuring active participation in school affairs, including improved information flow e.g. text messaging service to parents, Schoop, planning stored on central school NAS Drive or One Drive, school website updated regularly.

We will endeavour to reduce the burden of administration through effective use of ICT including general administrative communications and data transfer between schools, the LEA and central Government. We also will promote the effectiveness of management in information gathering, analysis, decision-making and communication through effective use of ICT.

In light of the Digital Competence Framework (DCF) being made available to school from September 2016, the school has strived to embed the framework and incorporate it into the curriculum and highlight in our planning. The ICT co-ordinator has helped with staff awareness and support this new development.

We will provide appropriate and efficient technical support to ensure the daily availability of the ICT resources.

---

## **Introduction**

The importance of Information and Communication Technology (ICT) prepares pupils to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. Pupils will use ICT as a tool for learning so providing more effective methods to discover and present ideas. Pupils use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination. Every child has the opportunity to learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of people, communities and cultures. Increased capability in the use of ICT promotes initiative and independent learning, with pupils being able to make informed judgements about when and where to use ICT to best effect, and to consider its implications for home and work both now and in the future.

This policy document sets out the school's aims, principles and strategies for the delivery of Information and Communication Technology (ICT) and e-Safety. This policy was developed in the Spring of 2019 by the ICT/e-Safety Coordinator. It was formally adopted by all staff and governors (who have each received a copy and signed an acknowledgement of this). All teaching students and new staff members will be requested to read and sign for the policy as they commence work in the school. This policy will be reviewed at regular intervals and updated as necessary by the ICT/e-Safety Coordinator. This policy is also available for parents on request. This policy is applicable to all that work within the school and any visiting guests who may use our IT equipment. Any violation of the policy may lead to disciplinary action or even criminal prosecution.

## **The Significance of Information and Communication Technology**

As well as being an important curriculum requirement, the ability to use IT effectively is a vital life skill.

We interpret the term Information Communication Technology to include the use of any equipment, which allows users to communicate or manipulate information electronically.

## **Aims and Objectives**

At Llangan Primary School, the aims of teaching ICT are for:

- The ICT provision meets the requirements of the Foundation Phase Curriculum and the National Curriculum.

- 
- Children, parents, staff, governors and the wide community have relevant and meaningful experiences using ICT.
  - Children have a growing awareness of how ICT is used in the world around them and of the benefits that it provides.
  - ICT is used to support problem solving and learning across the curriculum
  - Learners have equal access to ICT ensured by planning and differentiation
  - To ensure that the children can develop their literacy and numeracy skills through the use of IT

## Curriculum and Provision

Planning is undertaken at three levels:

**Long term** planning is based on the yearly teaching from the Computing Unlocked Scheme of Work.

**Medium term** planning is carried out half-termly. Teachers select their main teaching objectives from the yearly teaching programme to ensure a balanced ICT curriculum.

**Short term** planning is carried out weekly. These plans include learning objectives for the mental oral starter and the main activity, resources to be used, any differentiation, key vocabulary and learning style adopted.

Short term planning is monitored by the Headteacher, Deputy/ICT Subject Leader.

- Coverage and progression is ensured by long term planning, by using the 'Computing Unlocked' Scheme of Work.
- Opportunities for embedded ICT as a tool to support learning and teaching are identified in curriculum planning

### Foundation Phase

Work undertaken within the Early Years is guided by the requirements and recommendations set out under the Seven Areas of Learning. We give all the children ample opportunity to develop their understanding of ICT. We aim to do this through varied activities that allow them to use, enjoy, explore, practise and talk confidently about ICT.

## Resources

Resources for the delivery of the ICT curriculum are stored both centrally and in classrooms. Everyday hardware is kept in classrooms. Additional equipment and topic-specific items are stored centrally - Photocopying Room

---

Hardware is constantly updated, as new and relevant items become available. The ICT subject leader orders new resources after consultation with the staff.

- Resources are purchased and deployed effectively to meet the requirements of the Foundation Stage Curriculum and National Curriculum.
- An ICT asset register is maintained by the ICT Coordinator.

## Assessment and Monitoring

### Assessment and monitoring progress

At Llangan we are continually assessing our pupils and recording their progress. We see assessment as an integral part of the teaching process and endeavour to make our assessment purposeful, allowing us to match the correct level of work to the needs of the pupils, thus benefiting the pupils and ensuring progress.

- Observations, summative and formative assessment fully informs future planning
- Progress is assessed using the key objectives for ICT
- Children are encouraged to evaluate their own and others' work in a positive and supportive environment
- Teacher judgments are supported through agreement and a portfolio of evidence is kept to show standardisation.
- Information is shared with stakeholders through display, newsletters, reports and websites.

### The Digital Competence Framework

Digital competence is one of 3 cross-curricular responsibilities, alongside literacy and numeracy. It focuses on developing digital skills which can be applied to a wide range of subjects and scenarios.

The children develop these skills further and apply them in a cross-curricular way which addresses the expectations and requirements of the Digital Competency Framework (DCF).

The Framework, which has been developed by practitioners from Pioneer Schools, supported by external experts, has 4 strands of equal importance, each with a number of elements.

- Citizenship - which includes:
  - Identity, image and reputation
  - Health and well-being
  - Digital rights, licensing and ownership
  - Online behaviour and cyberbullying.

- 
- Interacting and collaborating - which includes:
    - Communication
    - Collaboration
    - Storing and sharing.
  
  - Producing - which includes:
    - Planning, sourcing and searching
    - Creating
    - Evaluating and improving.
  
  - Data and computational thinking - which includes:
    - Problem solving and modelling
    - Data and information literacy.

The school has already begun the process of familiarisation and implementation of the DCF through an addition of a hard copy with adjacent year groups being added to the planning files and staff highlighting the cross-curricular use in their weekly planning.

Specific guidance can be found at:

<http://learning.gov.wales/docs/learningwales/publications/160831-dcf-guidance-en-v2.pdf>

## **Cross Curriculum**

### **The contribution of ICT to other curriculum areas.**

ICT is taught mainly as a separate subject but every effort is made to link ICT with other areas of the curriculum. As a Key Skill we try and identify the technological possibilities across the curriculum at the planning stage. We also draw children's attention to the links between ICT and other curricular work so children see that ICT is not an isolated subject. In science pupils will, for example, use data handling skills to use spreadsheets and decide whether it is more appropriate to use a line graph or bar chart, and plot, interpret and predict from graphs.

In the Early Years, these links are more evident because of the less formal timetable.

### **Providing equal opportunities and teaching children with special needs**

---

At Llangan Primary School, we teach ICT to all children regardless of ability, gender, race, religion, or cultural differences, therefore providing a broad and balanced curriculum and promoting equal opportunities.

Teachers try to provide learning opportunities matched to the needs of children with learning difficulties, and work in ICT takes into account targets set for children in their Individual Education Plan (IEP's).

### **Display**

We recognise the important role display has in the teaching and learning of ICT by having ICT work displayed in the school. Every phase has an ICT display, where possible, which has vocabulary and other display materials that provide a visual support for the children's ICT skills.

## **Implementation and Monitoring**

### **Assessment and monitoring progress**

At Llangan we are continually assessing our pupils and recording their progress. We see assessment as an integral part of the teaching process and endeavour to make our assessment purposeful, allowing us to match the correct level of work to the needs of the pupils, thus benefiting the pupils and ensuring progress.

The subject leader for ICT is responsible for monitoring the standards of children's work and the quality of teaching in maths by observations, looking at planning and levelling examples of work. The subject leader keeps samples of children's work as part of a levelled portfolio in order to monitor standards throughout the school.

The role of the subject leader is also to support colleagues in the teaching of ICT, keeping informed about current developments in the subject and providing a strategic lead and direction within the school. The subject leader is also responsible for providing the Headteacher with an annual report which evaluates the strengths and weaknesses within the subject, feeding into an action plan which indicates areas for further improvement.

### **Continuity and Progression**

Class teachers are responsible for ensuring coverage of the ICT skills appropriate to their year group in their planning.

---

## Online Safety

When the Internet is being used, then the School's Acceptable Use Policy will always be strictly adhered to. Pupils will learn about the importance of e-Safety through their ICT lessons and in cross curricular contexts.

### The online safety policy

This policy applies to all members of the school (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital 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/committee Llangan Online Safety Group made up of:

- [Mr M Sinnett](#) - Deputy Headteacher / ICT and Online Safety Coordinator
- Staff
- Governors
- Digital Leaders

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

The policy will be monitored in the following ways:

- Informal discussion with staff and pupils
- Observation of ICT displays
- Collection of class ICT work in pupil folders / HWB accounts
- Classroom observation

### Schedule for Development/Monitoring/Review

This online safety policy was approved by the <i>Governing body/governors subcommittee on:</i>	
The implementation of this online safety policy will be monitored by:	<i>Mr M Sinnett - Deputy Headteacher</i>
Monitoring will take place at regular intervals:	<i>Yearly</i>

<p>The <i>Governing Body/governors subcommittee</i> will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:</p>	<p><i>Yearly</i></p>
<p>The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:</p>	<p><i>March 2020</i></p>
<p>Should serious online safety incidents take place, the following external persons/agencies should be informed:</p>	<p><i>Miss S Price (Headteacher), Mr M Sinnett (Deputy Headteacher/ ICT Coordinator) Governor responsible for Safeguarding When appropriate, the Child Exploitation Online Protection Command at the NCA.</i></p>

## **Roles and Responsibilities**

The following section outlines the online safety roles and responsibilities of individuals<sup>1</sup> and groups within Llangan Primary 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* 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 termly meetings with the online safety co-ordinator/officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering change control logs (if possible)
- reporting to relevant governors/sub-committee/meeting

### **Headteacher 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

<sup>1</sup> In a small school/college some of the roles described below may be combined, though it is important to ensure that there is sufficient "separation of responsibility" should this be the case.

---

responsibility for online safety will be delegated to the online safety co-ordinator.

- 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<sup>2</sup>
- The headteacher/senior leaders are responsible for ensuring that the online safety co-ordinator 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/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 headteacher/senior leaders will receive regular monitoring reports from the online safety co-ordinator.

**Online Safety Co-ordinator: Mr M Sinnett - Deputy Headteacher**

#### **The ICT and Online Safety Co-ordinator**

- leads the online safety group - the Digital Leaders.
- develops the use of eAware - to promote e-safety in the school by using a published package to track users.
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school/college 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 (or identifies sources of) training and advice for staff
- liaises with the local authority/relevant body
- liaises with the schools' technical staff
- receives reports of online safety incidents<sup>3</sup> and creates a log of incidents to inform future online safety developments.

- 
- attends relevant meeting/sub-committee of governors
  - reports regularly to headteacher/senior leadership team

### **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 agreement (AUA)
- they report any suspected misuse or problem to the Deputy Headteacher; online safety co-ordinator for investigation/action
- all digital communications with learners/parents and 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
- Learners understand and follow the online safety and acceptable use agreements
- learners 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 and implement current policies with regard to these devices
- in lessons where internet use is pre-planned learners 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

### **Designated senior person**

The designated senior person should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data<sup>4</sup>
- access to illegal/inappropriate materials

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

### **Online safety group**

The online safety group (Digital Leaders with the ICT/Online Safety coordinator) provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the online safety group will assist the online safety co-ordinator with:

- the production/review/monitoring of the school/college online safety policy/documents.
- mapping and reviewing the online safety curricular provision - ensuring relevance, breadth and progression
- monitoring network/internet/incident logs where possible
- consulting stakeholders - including parents/carers and the learners about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool

An online safety group terms of reference can be found in the appendices

### **Learners:**

- are responsible for using the school digital technology systems in accordance with the learner 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 and carers**

Parents and 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, Hwb, learning platform 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

### **Community Users**

Community users who access school systems/website/Hwb/learning platform as part of the wider school/college provision will be expected to sign a community user AUA before being provided with access to school/college systems.

#### **All users MUST NOT:**

- Transmit, retrieve, or store any communication of a discriminatory or harassing nature or materials that are offensive, obscene, violent, pornographic or sexually explicit
- Use or transmit abusive, profane or offensive language on or through Llangan's Internet, e-mail or messaging systems
- Seek to gain access to restricted areas of the network
- Knowingly seek to access data that is confidential unless authorised to do so.
- Introduce or, attempt to introduce any form of computer virus
- Carry out any other hacking activities

### **Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and learners 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 or tracking of pupils locations. 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. Llangan 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/college events for their own personal use (as such use is not covered by GDPR). 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 learners in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school/college policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, although the personal equipment of staff should not be used for such purposes unless it is necessary and deleted from their devices as soon as possible.
- 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 Llangan into disrepute.
- Learners must not take, use, share, publish or distribute images of others without their permission
- 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.
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of learners are published on the school/college website.
- Learners' work can only be published with the permission of the learner and parents or carers.

---

## **Data Protection**

Personal data will be recorded, processed, transferred and made available according to GDPR. For more guidance, please see the schools' GDPR Policy.

## **Communications**

This is an area of rapidly developing technologies and uses. A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the Llangan considered the following as good practice:

- The official school email service (Parent Pay and Office 365) is 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.
- 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, Schoop, learning platform) 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 KS1, while learners at KS2 and above will be provided with individual school email addresses for educational use.
- Learners should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school/college website and only official email addresses should be used to identify members of staff.

## **Social media**

With an increase in use of all types of social media for professional and personal purposes Llangan Primary's e-safety policy sets out clear guidance for staff to

---

manage risk and behaviour online. This ensures the protection of learners, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out by the Education Council of Wales (ECW) 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.

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

Llangan provides the following measures to ensure reasonable steps are in place to minimise risk of harm to 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 learners, parents and carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

#### **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, or

---

impacts on, Llangan has made it 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.
- The school permits reasonable and appropriate access to private social media sites.

### **Monitoring of Public Social Media**

- As part of active social media engagement, it is considered good practice to pro-actively 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.

School use of social media for professional purposes will be checked regularly by the senior risk officer and online safety group to ensure compliance with the social media, data protection, communications, digital image and video policies.

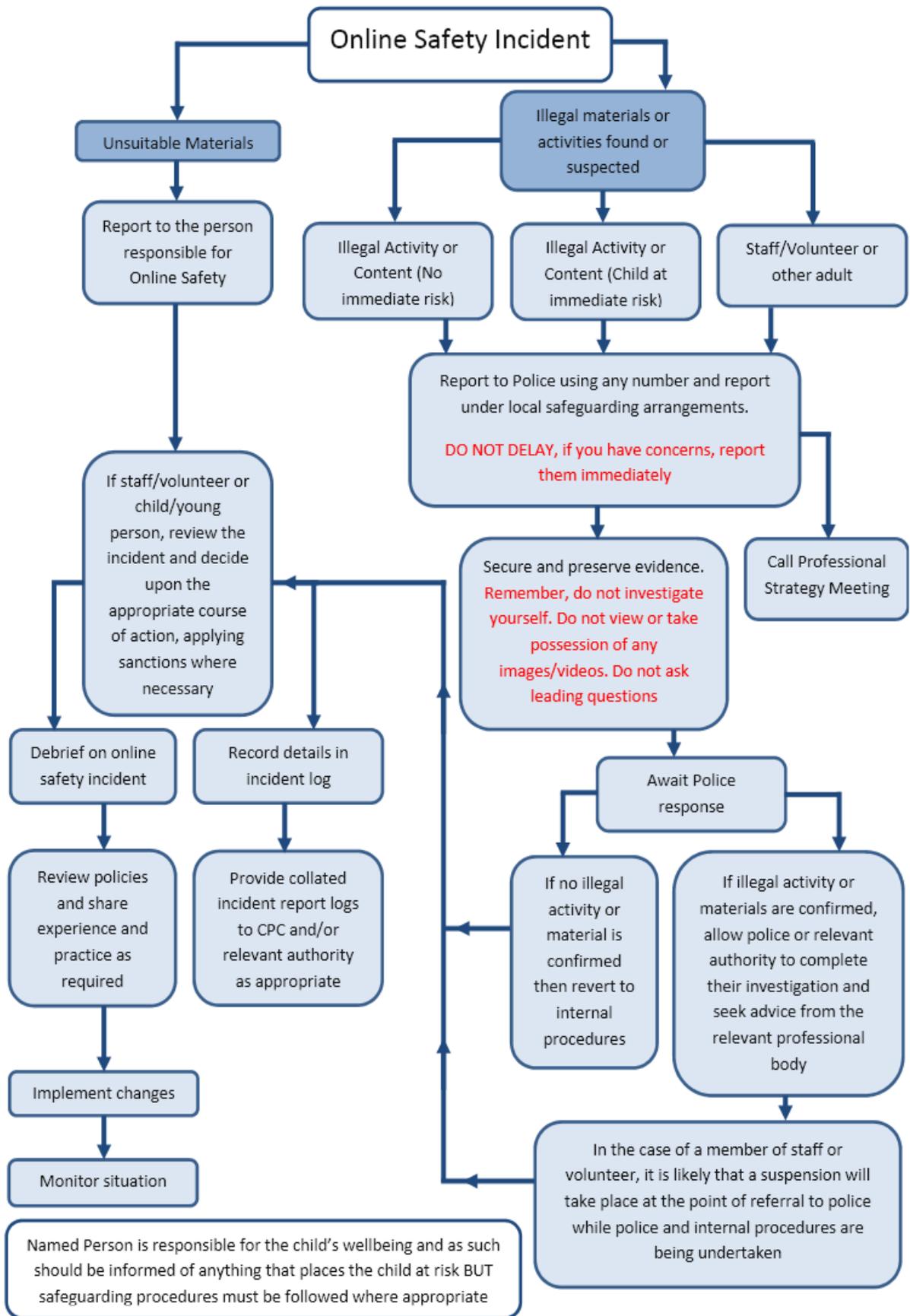
### **Unsuitable/inappropriate activities**

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. online 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.

**This policy will be reviewed at regular intervals and updated as necessary.**

**Mr M Sinnett (e-Safety Coordinator)**

**Date: 14/12/2018**



## APPENDIX 1: 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 school or outside school when using school equipment or systems. The school policy restricts usage as follows:

<u>User Actions</u>		Acceptable	Acceptable at certain times	Acceptable for nominated 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	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X		
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X		
infringing copyright				X		
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X		
Creating or propagating computer viruses or other harmful files				X		
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X		
On-line gaming (educational)	X					
On-line gaming (non-educational)		X				
On-line gambling				X		
On-line shopping / commerce			X			
File sharing			X			
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting e.g. YouTube	X					

---

## **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.

---

# Pupil Acceptable Use Policy Agreement

## 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 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.

Signed (child):..... Class .....

Signed (parent): .....

---

## 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 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 (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 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 (e.g. 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

---

## Acceptable Use Agreement for Community Users at Llangan Primary School.

This Acceptable Use Agreement is intended to ensure:

- that community users of school / academy digital technologies will be responsible users and stay safe while using these systems and devices
- that school / academy systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

### Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school / academy:

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, 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 school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- 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 if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

---

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.

Name:

Signed:

Date:

Copyright of these Template Policies is held by SWGfL. Schools / Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL ([esafety@swgfl.org.uk](mailto:esafety@swgfl.org.uk)) and acknowledge its use. Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in December 2018. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© South West Grid for Learning Trust Ltd 2016