Respect

Rydyn ni'n gallu llwyddo gyda'n gilydd

Nuture

Inspire

Together we can achieve

Ysgol Gynradd Llanmartin
Primary School

E-Safety Policy

Objectives of this Policy

- To inform all governors, teaching and non-teaching staff, pupils and parents of the schools' online safety policy intended to keep both children and the responsible adults safe online both in school and outside.
- To inform all governors, teaching, and non-teaching staff how to adhere to the school's online safety policy, what to do when they suspect a breach and the sanction the governing body will apply if a breach is proven.

Statement of Intent

We at Llanmartin Primary School are committed to providing a caring, friendly, and safe environment for all our pupils and staff so they can achieve their full potential in a relaxed and secure atmosphere. The internet offers a huge learning and teaching potential but, at the same time, a breach of internet safety guidelines e.g., through the use of Social Networking, external webpages or blog can lead to a breach of trust and even bullying and **Bullying of any kind is unacceptable** at our school. If bullying does occur, all pupils and staff should be able to tell and know that incidents will be dealt with promptly and effectively (see school policy on bullying). We are a TELLING school. This means that anyone who knows that bullying is happening is expected to tell a member of staff immediately.

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 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.

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 responsibility for Online Safety is delegated to the Digital Leader (Miss Hayley Cheney).
- The Headteacher and another member of the Senior Leadership Team / Senior Management Team are 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 Online Safety Coordinator are responsible for ensuring that the Online Safety Coordinator 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 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 support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator.

Online Safety Lead:

The Online Safety Lead

- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provides (or identifies sources of) training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with technical staff
- attends relevant meetings, including regular EAS Digital Network meetings and Newport schools digital network meetings
- reports regularly to Senior Leadership Team
- Hosts digital safety workshops for parents when necessary

Technical support: SRS are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets (as a minimum) the required Online Safety technical requirements as identified by the Local Authority and 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 is applied and updated on a regular basis
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Online Safety Coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of 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 Headteacher / Online Safety Coordinator for investigation / action
- All digital communications with students / learners / parents / carers should be on a professional level
- 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 (where allowed) 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 Safeguarding Person

The Safeguarding Officer should be trained in Online Safety issues and be aware of the potential for serious safeguarding issues to arise from:

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

Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online 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, website, social media, National and local Online Safety campaigns and 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
- Learner platforms such as Seesaw, Google Classroom and HWB

Policy Statements

Education – learners

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in Online Safety is therefore an essential part of the school's Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience. Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages across the curriculum. The Online Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Online Safety curriculum across a range of subjects and topic areas and regularly revisited
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and activities
- Learners should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in design making.

- Learners should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that 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.
- Where learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – parents / carers

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, learning platforms, HWB
- Parents / Carers workshops
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. https://hwb.wales.gov.uk/ www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

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

- A planned programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements.
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events by reviewing guidance documents released by relevant organisations.

- This Online Safety policy and its updates will be presented to and discussed by staff in development sessions.
- The Online Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

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

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents

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 / carers and students / 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. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate 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 e.g. 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. 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 policies concerning the sharing, distribution and publication of those images. Those images should only be taken on

school equipment, if they have to be taken on personal equipment then they will be deleted immediately after use.

- 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 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 blogs, particularly in association with photographs.

Communication technologies

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

- the official school e-mail service (HWB) may be regarded as safe and secure and is monitored. Users should be aware that e-mail 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 (e.g., by remote access)
- Users must immediately report to the nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and learners or parents/carers (e-mail, chat, learning platform, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems.
- Personal e-mail addresses, text messaging or social media must not be used for these communications
- Whole class/group e-mail addresses may be used at Progression Step 1, while learners at Progression Step 2 and above will be provided with individual school e-mail (Google) addresses for educational use.
- Learners should be taught about online safety issues, such as the risks attached to the sharing of personal details.
- Learners should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff

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. Core messages should include 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 Workforce Council (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.

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

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 learners through:

- ensuring that personal information is not published
- Training being provided including acceptable use, social media risks, checking of settings, data protection and 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.

When official school social media accounts are established, there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts
- Systems for reporting and dealing with abuse and misuse

- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- 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.

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 / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store

screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form (except in the case of images of child sexual abuse – see below)

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

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

The Head teacher, Mrs V Curtis, is the child protection officer but all staff are responsible for implementing this policy. All stakeholders have been consulted in writing this policy and information regarding this policy circulated to parents and made available for all interested parties via the school website.

This policy will be shared with all staff and any new member of staff will receive a copy as part of the induction training. The policy will be reviewed annually.

This policy was updated and taken to the Governing Body during Autumn Term 2022 and will be reviewed again during Autumn Term 2024.

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Think then Click

These rules help us to stay safe on the Internet

We ask permission before using the internet.

We only use websites our teacher has chosen.

We tell an adult if we see anything we are uncomfortable with.

We immediately close any webpage we are uncomfortable with.

We only email people an adult has approved.

We send e-mails that are polite and friendly.

We never give out personal information or passwords.

We never arrange to meet anyone we don't know.

We do not open e-mails sent by anyone we don't know.

We do not use Internet chat rooms.