The Llewellyn School Policies and Procedures

Online Safety & Social Media Policy

Policy Reviewed by:	Suzy Hollett (HR Manager)
Date:	23/01/2024

Policy Verified by:	Sara Llewellyn (School Leader-CEO)
Date:	23/01/2024

Date for Next Review:	01/01/2025

Llewellyn School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones, or games consoles.

Llewellyn School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

Llewellyn School has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff, and enhance management functions.

Llewellyn School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of Llewellyn School online safety policy is to:
Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that the school is a safe and secure environment.

- Safeguard and protect all members of the school community online.
- Raise awareness with all members of the school community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.
- This policy applies to all staff including the school Governors, teachers, support staff, external contractors, visitors, volunteers, and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff 'in this policy) as well as children and parents/carers.
- This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets, or mobile phones.
- This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding, anti-bullying, behaviour, and relevant curriculum policies including Sex and Relationships Policy

Key responsibilities for the community

The key responsibilities of the school senior management team are:

- Developing, owning, and promoting the online safety vision and culture to everyone, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- Ensuring all members of staff receive regular, up-to-date, and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate and developmentally appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records, using them to inform and shape practice.
- Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local, and national support.
- To ensure a member of the School Governors of Llewellyn School is identified with a lead responsibility for supporting online safety.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

The key responsibilities of the Designated Safeguarding Lead

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up to date with current research, legislation, and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour, e.g., Safer Internet Day.

- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school/setting lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms. Currently recorded on CPOMs.
- To report to the school management team, School Leader, School Governors of Llewellyn School, and other agencies as appropriate, on online safety concerns.

The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies
- Taking responsibility for the security of school/setting systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

The key responsibilities of children and young people are:

- At a level that is appropriate to their individual age, ability, and vulnerabilities:
- Contributing to the development of online safety policies as appropriate
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong and supporting others that may be experiencing online safety issues.
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any technology and behaving safely and responsibly to limit those risks.

The key responsibilities of parents and carers are:

- Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.

- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school/setting online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Publishing images online

- The school will ensure that all images and videos shared online are used only on the school website/Facebook.
- The school will ensure that all use of images and videos take place in accordance with other policies and procedures including data security.
- Written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school address, email, and telephone number. Staff or pupils' personal information will not be published.
- The School Leader / CEO will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the school's guidelines for publications including accessibility, respect for intellectual property rights, privacy policies and copyright.
- Pupil's work will be published with their permission or that of their parents/carers.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

Managing emails

- All members of staff are provided with a specific school/setting email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g., sensitive, or personal information) will only be sent using secure and encrypted email.

- Access to school email systems will always take place in accordance with data protection legislation and in line with other appropriate school policies e.g., confidentiality.
- Members of the community must immediately tell the DSL if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of Llewellyn School community and exist to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger, and many others.
- All members of the school community will be encouraged to engage in social media in a positive, safe, and responsible manner always.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the school community.
- All members of the school community are advised not to publish specific and detailed private thoughts, concerns, pictures, or messages on any social media services, especially content that may be considered threatening, hurtful, or defamatory to others.
- The use of social networking applications during school hours for personal use is not permitted.
- Inappropriate or excessive use of social media during school/work hours or whilst using school/setting devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of the school community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour, and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken, and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour, and safeguarding.

Official use of social media

- Llewellyn School official social media channels are:
  https://twitter.com/LlewellynSchool
  https://www.facebook.com/thellewellynschool

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g., increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the CEO / School Leader.
- All communication on official social media platforms will be clear, transparent, and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common-law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and child protection.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Public communications on behalf of the school will, where possible, be read and agreed by at least one other colleague.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- All communication between staff and members of the school community on school business will take place via official approved communication channels.
- Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the CEO / School Leader.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social

media use is compatible with their professional role and is in accordance with school's policies and the wider professional and legal framework.

- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.
- Members of staff are encouraged **not** to identify themselves as employees of Llewellyn School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school/setting and to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of the school on social media.
- School email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the school/settings social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

Appendix A:
Online Safety (e-Safety) Contacts and References

Kent Support and Guidance
Kent County Councils Education Safeguards Team:
www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
Kent Online Safety Support for Education Settings

- Education Safeguarding Adviser (Online Protection)
- e-Safety Development Officer
- esafetyofficer@kent.gov.uk Tel: 03000 415797

Kent Police:
www.kent.police.uk or www.kent.police.uk/internetsafety
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

- Kent Public Service Network (KPSN): www.kpsn.net
- Kent Safeguarding Children Board (KSCB): www.kscb.org.uk
- Kent e-Safety Blog: www.kentesafety.wordpress.com
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk

National Links and Resources:

- Action Fraud: www.actionfraud.police.uk
- CEOP (Child Exploitation and Online Protection): www.ceop.police.uk
- ChildLine: www.childline.org.uk
- Child net: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- Know the Net: www.knowthenet.org.uk
- Net Aware: www.net-aware.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
- Parent Port: www.parentport.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/
- Think U Know: www.thinkuknow.co.uk
- Virtual Global Taskforce: www.virtualglobaltaskforce.com
- UK Safer Internet Centre: www.saferinternet.org.uk
- 360 Safe Self-Review tool for schools: https://360safe.org.uk/

Online Compass (Self review tool for other settings):
http://www.onlinecompass.org.uk/