UK Council for Internet Safety

Llywodraeth Cymru
Welsh Government

Online safety

Five key questions for governing bodies to help challenge their schools and colleges to effectively safeguard their learners

Online safety

Five key questions for governing bodies to help challenge their schools and colleges to effectively safeguard their learners

Audience

This document has been produced by Welsh Government and the UK Council for Internet Safety (UKCIS) to support governing bodies of schools and colleges in Wales.

It might also be of interest to local authorities, diocesan authorities, Governors Wales, and any other interested parties that have a lead responsibility for online safety.

Overview

This document is to support governing bodies to undertake their safeguarding duties as a governing board. It can be considered a supporting document to the Welsh Government's *Keeping learners safe* statutory guidance, which sets out roles and responsibilities in respect of safeguarding children. This includes supporting schools to provide a safe, responsible and supportive environment to learn and prevent access to inappropriate or harmful content.

Action required

No action is required. This document is a guide only, intended to support governing bodies to ensure that good practice around online safety policy and provision is operational in their school or college.

Further information

Enquiries about this document should be directed to:
Digital Resilience in Education Branch
Digital Learning Unit
Digital and Strategic Communications Division
Welsh Government
Cathays Park
Cardiff
CF10 3NQ
e-mail: hwb@gov.wales

Additional copies

This document can be accessed from the Hwb website at
hwb.gov.wales/zones/online-safety

Contents

Five key questions

1. **Does the school/college have an up to date online safety policy and acceptable use policy in place? How does the school/college assess that they are clear, understood and respected by all children and staff?**

What to look for?

- Systematic and documented regular review of safeguarding policies, including online safety, at least on an annual basis.
- Evidence that online safety policies are readily available and clearly communicated (e.g. school/college website, staff handbooks, posters, etc.).
- Learners, staff and parents/carers are aware of, and respect, online safety rules and expectations.

What good practice looks like?

- Collaborative production and review of policies, for example, evidence of the active use of learners' and parents'/carers' views as well as evidence of appropriate cognisance of national and international standards of online safety.
- Evidence of monitoring and evaluation processes to ensure understanding of, and adherence to, online safety policies.
- Learners, staff and parents/carers are alert to online safety behaviour and expectations, including the acceptable use of technologies and the use of mobile technology.
- The school/college child protection policy recognises peer on peer abuse concerns which can take place online.
- Linked to and a part of other policies, such as safeguarding and child protection, learners' behaviour (including anti-bullying), staff code of conduct.
- Policies do not use and, where appropriate, actively challenge 'victim blaming' language and recognise that children are never responsible for the harm which they may experience, especially given the online context/pervasive nature of social media technology.

When should you be concerned?

- There are minimal or no online safety policies in place.
- Policy is generic and not specifically relevant to the learners needs in the school/college.
- Online safety policies are being reviewed infrequently or not at all.
- Policies exist but are not publicised to the school/college body and/or are not known by staff, learners and parents/carers.

2. What mechanisms does the school/college have in place to support learners, staff and parents/carers facing online safety issues?

What to look for?

- Online safety clearly recognised as a safeguarding issue within the roles and responsibilities of all staff in the school/college with overall responsibility held by the designated senior person (DSP) for child protection.
- Whole school/college approach, in which robust reporting channels are well-defined, clearly understood and consistent and known by all school/college staff, learners and parents/carers.
- Clearly documented and visible procedures for responding to different online risks, e.g. sexting, upskirting, online bullying and online grooming.
- Learners, staff and parents/carers understand the sensitive nature of online abuse as well as the rights of individuals.
- Links into other relevant policies and procedures, e.g. whistleblowing, managing allegations, complaints, etc.
- Leadership staff are aware of and understand the decisions made by the school/college in respect of implementing appropriate filtering and monitoring.
- Regular review of monitoring and filtering provisions as part of safeguarding responsibilities, e.g. evidence of communication between technical staff and DSPs.

What good practice looks like?

- Regular review of provision using the 360 Safe Cymru self-review tool and inclusion of the 360 review in team meetings.
- Online reporting mechanisms for learners and parents/carers.
- All staff are aware of sources of support for online safety issues, such as the Professionals Online Safety Helpline, Reporting Harmful Content, CEOP and Internet Watch Foundation (URLs are listed in the 'Further sources of support for online safety issues' section).
- The DSP and deputies have the appropriate skills and are trained to deal with the various risks related to online activity. There may be additional nominated members of staff who support this area with their expertise.
- All staff should receive appropriate safeguarding and child protection training, including online safety, which is regularly updated.
- Planned and effective peer support strategies, e.g. reporting mechanisms/escalation processes supported by all school/college staff.
- Auditing of online behaviour and risks which provides baseline information from the learners about the levels and types of online issues prevalent in the school/college.
- Learners contribute to the development of the provision through their own knowledge and expertise, peer activities, and learner voice activities.

- Regular evaluation of reporting channels and response procedures.
- Online safety information/data highlighted within the headteacher's report to the governing body.
- Appropriate filtering and monitoring decisions are regularly reviewed in line with the school/college's needs and relevant information is clearly communicated to staff, learners and parents/carers.

When should you be concerned?

- There are no reporting channels in place, or they are unclear/inconsistent.
- There are no recording processes to enable the school/college to identify and monitor concerns.
- Learners and parents/carers unaware of or have a lack confidence in reporting channels.
- Staff are unclear of how to support learners and parents/carers with online safety concerns.
- Appropriate filtering and monitoring approaches are not in place, and/or there is a lack of understanding of the decisions made with respect to appropriate filtering and monitoring by the leadership team.

3. How do you ensure that all staff receive appropriate, relevant and regularly updated online safety training?

What to look for?

- Training events on Hwb's Online safety zone.
- Training which improves staff knowledge of, and expertise in, safe behaviours and appropriate use of technologies.
- Audit of the training needs of all staff.
- Online safety training as an integral part of the required, at least annual, safeguarding training for all staff. Online safety training as an integral part of induction for all new staff.
- Online safety training coordinated by the DSP.
- Evidence that the DSP (and their deputies) has ensured that their knowledge and skills regarding online safety is robust.

What good practice looks like?

- DSP and their deputies have a higher level of training, knowledge and expertise on online safety issues, with clearly defined responsibilities related to online safety provision for the school/college community.
- Expertise in online safety is developed across a pool of staff, to ensure transfer and sustainability of knowledge and training.
- Online safety training clearly established within the school/college's wider safeguarding training.
- Training content updated to reflect current research and advances in technology as well as local policy and procedures.
- Online safety training is given to all new staff as part of induction.

When should you be concerned?

- DSP and their deputies lack appropriate training and authority in online safety.
- There is no recognised individual/group for online safety or they lack appropriate training and authority.
- There is a lack of training for all staff, or training is out-of-date.
- There are some staff that have no online safety training.
- Regular updated training (at least annual) is not undertaken.
- Training on online safety does not meet the needs of staff.
- Training based on outdated resources/materials, or materials which lack accuracy.
- Lack of clarity on who coordinates staff training.

4. Describe how your school/college provides the learning required to educate children and young people to build knowledge, skills and confidence with regard to online safety.

What to look for?

- Implementation of the Digital competence framework (DCF), with digital skills, knowledge and attitudes embedded across the curriculum and integrated into lessons.
- Planned online safety education programme which:
  - is taught across all age groups and progresses as learners grow and develop
  - is recurring and progressive as opposed to a one-off online safety session
  - supports learners in developing strategies for navigating the online world and developing resilience
  - is embedded across the curriculum
  - incorporates/makes use of relevant national initiatives and opportunities such as Safer Internet Day and Anti-bullying week.
- Use of appropriate and up-to-date resources.
- Resources, including visitors from external providers used appropriately to support and compliment internal provision.
- Accessible to learners at different ages and abilities, such as learners with additional learning needs (ALN), or those with English as an additional language.
- Learners are able to recall, explain and actively use online safety education.
- Teachers have access to appropriate training, ensuring expertise and understanding underpins their teaching.

What good practice looks like?

- Online safety is embedded throughout the school/college curriculum. This means that the opportunity to develop the knowledge, skills and confidence of learners, on issues related to online safety, are planned into all relevant lessons such as in personal and social education (PSE), relationships and sexuality education (RSE) and Computer science.
- Regular review of online safety across the curriculum to ensure its relevance to learners.
- The learning activities provided include a diverse range of topics relating to online safety that reflects current and emerging issues.
- Learners are regularly consulted through appropriate channels (learner groups, forums, etc.) for input on the online safety issues relevant to them.

When should you be concerned?

- Ad-hoc/one-off sessions on online safety, such as sessions only delivered through assemblies.
- Content used is inaccurate, irrelevant or out of date and/or inappropriate for the age/ability of the learner.
- Resources/materials used with learners rely on fear, shock or victim blaming approaches.
- The programme of study in place is not progressive or sustainable, e.g. substantial reliance on external providers/visitors to deliver online safety education and/or is delivered in response to a specific issue.
- No means to evaluate the effectiveness of provision and assess learners' understanding in the area.
- The school/college is failing to have regard for online safety as part of its relationships and sexuality provision.
- The school/college does not use the 360 degree safe Cymru tool for regular review of its provision.
- The school/college is not embedding digital competence across the school curriculum.

5. How does the school/college educate parents/carers and the whole school/college community with online safety?

What to look for?

- Regular communication, awareness-raising and engagement on online safety issues and reporting routes, such as the school/college websites, social media platforms and newsletters.
- Regular opportunities for engagement with parents/carers on online safety issues such as awareness workshops.
- Sharing good practice with other schools in clusters and/or the local authority.

What good practice looks like?

- Interactive engagement with parents/carers, with the aim of building skills and confidence to support their children and young people in dealing with online risks, as well as general awareness on online safety issues.
- Regular and relevant online safety resources and sessions offered to parents/carers. Relevant resources will tackle key online risks and behaviours displayed by learners at different ages in the school/college.
- Evidence of learners educating parents/carers and members of the community.
- Online safety information available in a variety of formats, such as for those with English as an additional language.
- A willingness to engage with other schools and local agencies to promote, share and learn from good practice and expertise.

When should you be concerned?

- There is no or only minimal awareness-raising on online safety issues.
- There is no online safety engagement with parents/carers, the wider community, other schools or organisations.
- Recurrent concerning online behaviours among learners (such as younger children playing games aimed towards older adolescents and adults).

Supporting your school/college to improve online safety practice

360 degree safe Cymru

The 360 degree safe Cymru audit tool can be accessed from the main menu when logged in to Hwb. It supports schools to review their online safety policy and practice. You should check that the school has an account and, if they do, when they last used the tool.

Online safety zone on Hwb

The Online safety zone on Hwb hosts resources for learners, parents and carers, teachers and governors on a range of specific online issues, including online bullying, online reputation and misinformation.

There are also more general resources available, such as the *How to keep myself safe online (Governors)* playlist, which provides advice on how you can support your learners, school and each other to stay safe online.

Training

Online safety training
Educational practitioners and professionals can register for online safety training and events on the Online safety zone on Hwb. Digital regional consortia leads will be able to advise if there are any training events taking place in your area.

Keeping learners safe modules
Supporting the statutory guidance *Keeping learners safe*, there are three safeguarding modules available for teachers and staff. There are two further modules (4 and 5) which solely focus on online safety issues. Module 4 is for teachers and Module 5 is for governors.

Related Welsh Government documents

- *An online safety action plan for children and young people in Wales*
- *Draft keeping learners safe guidance*
- *Recommended web filtering standards for schools in Wales*
- *Digital competence framework guidance*
- *Relationships and sexuality education in schools*

Further sources of support for online safety issues

UK Safer Internet Centre
www.saferinternet.org.uk/

Professionals Online Safety Helpline
www.saferinternet.org.uk/helpline/professionals-online-safety-helpline

CEOP: Reporting online sexual abuse or concerning online communication
www.ceop.police.uk/ceop-reporting/

Internet Watch Foundation
report.iwf.org.uk/en

Reporting harmful content
www.saferinternet.org.uk/helpline/report-harmful-content

SchoolBeat Cymru
schoolbeat.cymru/

NSPCC
www.net-aware.org.uk/

The UKCIS Education Working Group is comprised of the following organisations: