



Monmouthshire Pupil Referral Service

Online Safety (including Teaching Online) Policy

Document Control	
Document author	Jake Parkinson
Statutory status	
Website status	
Approved by	Management Committee
Date approved	December 2025
Approval cycle	Biannual
Next review date	December 2027

Document history			
Version	Date	Reviewer	Note of revisions

Introduction

This policy applies to all members of the school community (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. It also applies to the use of personal digital technology on the school site (where allowed).

This Online Safety Policy outlines the commitment of the Monmouthshire Pupil Referral Service (PRS) to safeguard members of our school community online in accordance with principles of open government and with the law. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

The Monmouthshire PRS will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding. Online safety is a core part of safeguarding in the era in which we now live.

The Monmouthshire Pupil Referral Service has a Digital Champion who works closely with the DSL and DDSs. All staff are trained in online safety issues. Staff work together to develop a planned and coordinated online safety education programme, through the PRS curriculum. Staff ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies about these devices

Online Learning

Where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the [Live Streaming and Video Conferencing safeguarding principles and practice for education guidance](#).

Key information from this document and adopted by the Monmouthshire PRS is that:

- all video-conferencing or live-streamed lessons/sessions should be carried out via Hwb using Microsoft Teams or Google Meet, rather than an external provider, or the school/setting's own implementation of Google/ Microsoft 365
- the practitioner uses a school/setting-issued device. School or setting staff should not use their own personal equipment under any circumstances

Location, camera and audio settings

It is essential to carefully consider location, audio and camera settings to always maintain a professional and responsible disposition. This is particularly important when practitioners or learners are at home.

If a practitioners should ensure that any online lessons are delivered from an MCC building, with other staff members present. Staff will ensure that the risk of interruptions are reduced. Staff carefully consider what is in view of the camera or use blur or an MCC or Monmouthshire approved background if needed. Staff are mindful that not all learners will want to switch their camera on. The use of a headset with microphone (like those available with many mobile phones) is recommended for audio clarity. Practitioners choosing to live-stream should continue to work in the same professional manner as they would in the classroom. Practitioners must adhere to professional standards of dress when in front of the camera, be conscious that in an online environment remarks are being heard by a number of learners and could be easily misconstrued and ensure at the close of the lesson, the session is ended for all participants, ensuring learners are not left alone and unsupervised in a lesson/session the practitioner has left. Staff should also be mindful of the need for confidentiality; especially if live streaming a lesson from a venue where other adults or children are present.

Practitioners or staff should try to avoid undertaking a video-conferencing lessons where only one learner is present, but we are aware that this is sometimes the case. undertake a video-conferencing lesson where only one practitioner and one learner are present. If it is not practical to have a second staff member present at the lesson/session, the practitioner should record the lesson/session to safeguard both learners and staff. If staff have concerns regarding the presentation of a learner online, or a learner suddenly leaves a session unexpectedly, parents/carers should be contacted as soon as possible.

Practitioners should join the lesson/session before the scheduled time to ensure a proper connection and review the lesson plan, so they feel prepared for an effective lesson/session.

There may be exceptional circumstances (such as counselling sessions, appointment with an Education Psychologist or ALNCo) where the nature of the conversation requires a confidential one-to-one session with a practitioner, as would be normally conducted in a school/setting. Each individual session must be considered and agreed by the headteacher and the Designated Safeguarding Lead of the Monmouthshire PRS. Consent must also be granted and recorded from the learner's parents/carers. Written acknowledgement of the session should be placed on file in accordance with local data storage arrangements.

As a video-conferencing or live-stream recording constitutes personal data, you must comply with the MCC data protection policies and GDPR regulations.

If you intend on recording a lesson to share with learners later, this should be done as an asynchronous activity without learners being present in the recording.

Please note: any recordings must not be used for any teacher-evaluation purpose.

Please set out acceptable behaviours and expectations from the outset, ensuring an effective and orderly lesson or session. Staff will use the Monmouthshire PRS expectations document and Relationships and Behaviour Policy to support this.

Staff will immediately address and report incidents of online-bullying, sexual harassment, discrimination, hatred etc. Staff model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Use of mobile phones and emails at school

Mobile phones should only be used at break or lunch times, or when directed by staff, for example taking images of evidence of work or using calculator functions for EOTAS medical learners. If pupils use mobile phones in school outside of these times, we will follow our Rewards and Expectations guidelines. Under no circumstances should pupils take pictures of other learners or staff members on their phones. Pupils should not bring any other personal devices to school. Pupils must not use personal emails for school business, and similarly they should not use their Hwb emails for personal emails.

The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school

safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.

- all members of the school community will be made aware of the need to immediately report online safety issues/incidents.
- reports will be dealt with as soon as is practically possible once they are received.
- if there is any suspicion that the incident involves child abuse images, any other illegal activity or the potential for serious harm, the incident will be escalated through the normal school safeguarding procedures and the police informed. In these circumstances any device involved should be isolated to support a potential police investigation. In addition to child abuse images such incidents 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.
- any concern about staff misuse will be reported immediately to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of the Management Committee and the local authority

As long as there is no suspected illegal activity, staff may check devices as necessary, ensuring that any checks are done by senior members of staff. Staff will never ask to view any imagery that could possibly constitute child abuse on a school or learner's device.

Parents/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. Enhancing digital resilience in education: An action plan to protect children and young people online (November 2022) states: "We are committed to nurturing and promoting the safe and positive use of technology to children and young people by building a strong architecture around the child where professionals are skilled and families are aware of how to support children in their online lives. We seek to foster a protective environment for our children and young people by supporting families, practitioners, governors and other professionals creating a culture where keeping children safe online is everyone's business." We will support parents/carers to keep their children safe online.

When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure. In the event of any social media issues that the school is

unable to resolve support may be sought from the Professionals Online Safety Helpline.

Staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying 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 inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. Staff educate young people to 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 (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, 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, storage, distribution and publication of those images. Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes. Care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that may be embarrassing for learners or the school. 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. Permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes.

GDPR

The school follows the GDPR guidelines of the local authority and all staff undertake mandatory GDPR training on a regular basis. The headteacher is the Data Protection Officer (DPO). The school reports any relevant breaches to the Information Commissioner within 72 hours of becoming aware of the breach as required by law.

Staff guidance states:

1. Lock your computer when you are away from it

2. Maintain a clear desk policy. Make sure that nothing is left on your desk when you are not there. This is especially for anything that refers to a child or a member of staff or could be used to identify a child or a member of staff. This applies even if your office or classroom is locked.
3. Lock all sensitive data away. Data about children or a member of staff must be locked away.
4. Shred sensitive data that is no longer needed. Do not use the bins for sensitive data. It must be shredded. Do not keep sensitive data for longer than is needed, shred straight away.
5. Store information about children on school systems – don't store this anywhere else.
6. Never share a photo or video of a child on the PRS website or social media without checking for consent.
7. Only take hard copies of sensitive data off site if essential. If essential, ensure the information is secure and that it is only kept off site for the essential time needed.

Acceptable Use of IT

Access

Do not use school information systems for private purposes

Do not disclose any of your passwords or security information to anyone else

Do not install any software or hardware without permission from the Head of the PRS

Respect intellectual property right and adhere to the Data Protection Act 2018

Do not attempt to bypass any computer or network security settings

Internet

Ensure all electronic communications, including email, are compatible with your professional role

Only use school email systems to communicate with parents/carers and pupils

Only use Google Classroom, Microsoft Teams or Outlook email to communicate with parents/carers or pupils

Ensure social network privacy settings prevent others viewing my personal details and materials and ensure that I never accept, or request invites or friend requests from any pupils, past pupils, or parents/carers online.

Always promote e-safety with pupils

Report any incidents of concern regarding children's safety to the Designated Safeguarding Leads (as per Safeguarding policy)

Do not use work email address to sign up for any social networking sites or other sites other than those used within your professional role

Do not open any attachments, using work email address, from any unknown sources

Staff must take care when using social media and ensure that they do not bring themselves, Pupil Referral Service or Monmouthshire County Council into disrepute.

Staff must not share photos/images of learners on social media or discuss the service on any social media platforms

Storage

Only store school related or educational data, files and images on the Share Point and/or Hwb.

Use the VLE / Hwb only to transfer files between home and school

Any photographs/video taken of pupils or staff and use of afterwards will be done with their permission.

Remove any images or video footage of pupils from personal devices (if used) before leaving work, and do not process, edit or open them on a personal computer at home.

Report any loss of personal data immediately to our Data Protection Officer, Jake Parkinson (Head of Monmouthshire PRS)

Use of equipment

Do not use mobile phone or personal device for anything other than work purposes during lesson time

Guide and direct IT use for pupils

Report technical issues / damage as soon as possible to the PRS Administrator, Callan Radnovich at CallanRadnovich@monmouthshire.gov.uk

Cyberbullying

Follow Monmouthshire PRS procedures for antibullying

Advise pupils to keep evidence of cyber bullying by taking screen shots, saving emails and texts.

Cyber Attacks

The school, in partnership with their education technology support partner the Shared Resource Service (SRS), has an effective backup and restoration plan in place in the event of cyber-attacks.

Policy Review

The impact of this policy and our practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and the Management Committee.

This policy was approved by the Management Committee

Signed: *L Wilce* Chair of the Management Committee

Date:03.12.25.....

Signed:Jake Parkinson..... Head of the Pupil Referral
Service

Date:03.12.25.....