

DARLAND HIGH SCHOOL

Online Safety Policy

2026-2027

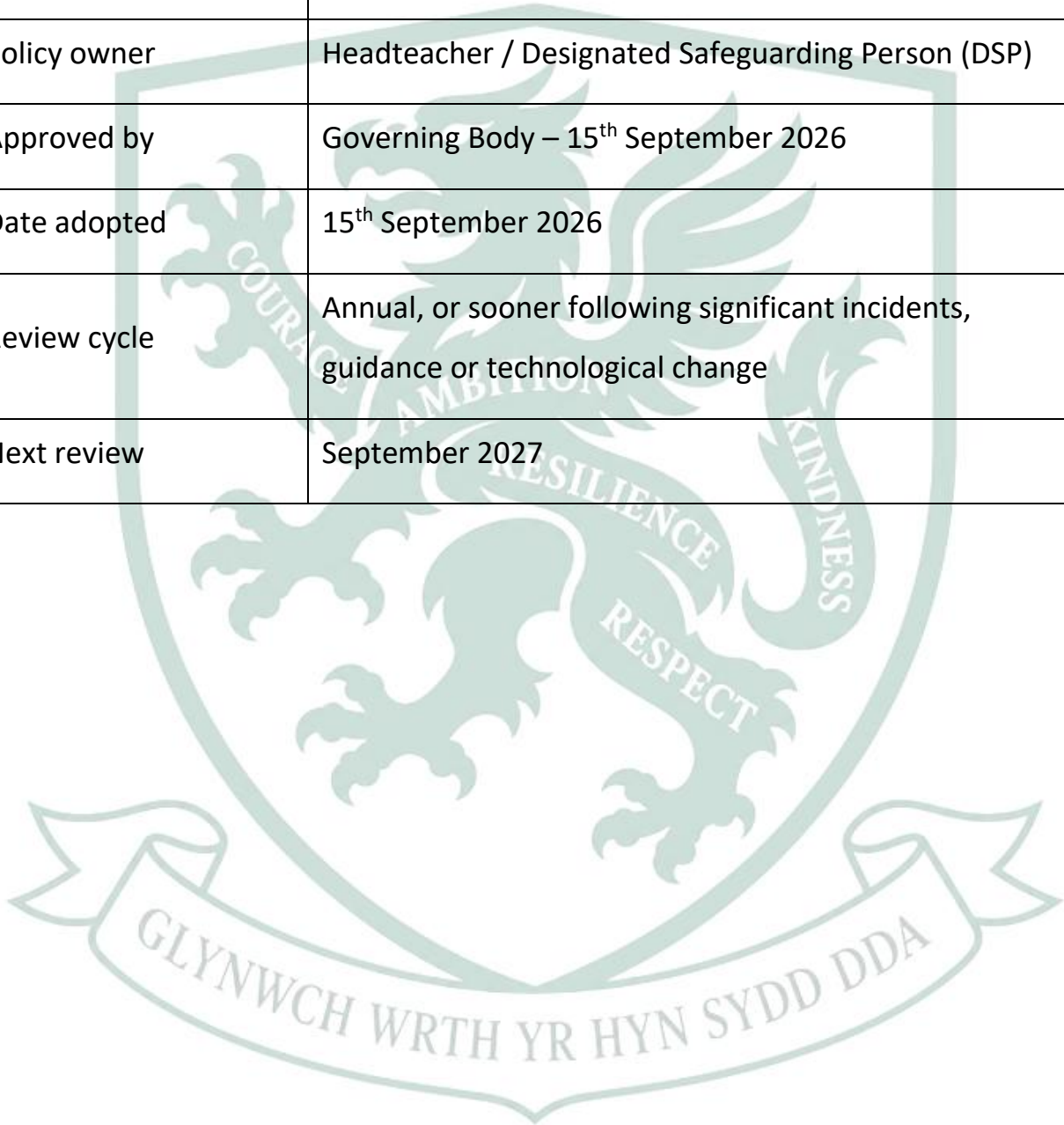
Acronyms:

- **DSP** – Designated Safeguarding Person
- **ICT** – Information and Communication Technology
- **MFA** – Multi-Factor Authentication
- **PSE** – Personal and Social Education
- **SLT** – Senior Leadership Team
- **HR** – Human Resources
- **CEOP** – Child Exploitation and Online Protection
- **SHARP** – the school's online reporting/communication system
- **URL** - Uniform Resource Locators (website address)
- **TBC** – To Be Confirmed

Policy statement

Online safety is a safeguarding responsibility. Darland High School is committed to enabling learners and adults to use digital technology safely, responsibly, respectfully and effectively, while protecting members of the school community from online harm.

Policy information	Details
School	Darland High School
Policy owner	Headteacher / Designated Safeguarding Person (DSP)
Approved by	Governing Body – 15 th September 2026
Date adopted	15 th September 2026
Review cycle	Annual, or sooner following significant incidents, guidance or technological change
Next review	September 2027



Courage • Ambition • Resilience • Respect • Kindness

1. Purpose and scope

This policy sets out Darland High School's approach to online safety and the safe and responsible use of digital technologies. It is based on the 360 safe Cymru Online Safety Policy framework and has been adapted into a school-specific working policy for a secondary school context.

It applies to all members of the school community, including staff, learners, governors, volunteers, parents and carers, visitors, contractors and community users who access or use school digital systems. It also applies to personal digital technology used on the school site where permitted, and to online behaviour outside school where it affects a learner, member of staff or the school community.

Core principle

Incidents of misuse or breaches of this policy will be addressed through the school's safeguarding, behaviour, anti-bullying, staff disciplinary and other relevant procedures. Where there is suspected illegal activity or a risk of significant harm, safeguarding procedures take precedence and external agencies will be involved as appropriate.

2. Aims

- protect learners and adults from online harm and ensure that online safety is understood as part of safeguarding;
- develop digitally resilient learners who can recognise risk, make informed choices, seek help and recover when things go wrong;
- set clear expectations for acceptable and responsible use of school systems, devices, networks and online services;
- ensure that filtering, monitoring, technical security and data protection arrangements support a safe learning environment;
- provide clear routes for reporting, recording and responding to online safety concerns;
- promote respectful, lawful and responsible online behaviour, including beyond the school site where it affects the school community;
- support staff, governors, parents and carers to understand their role in keeping learners safe online.

3. Links with other school policies

This policy should be read alongside the school's Safeguarding and Child Protection Policy, Behaviour for Learning Policy, Anti-Bullying Policy, Data Protection arrangements, Staff Code of Conduct, Acceptable Use Agreements, complaints and whistleblowing procedures, and any technical security or mobile device guidance.

4. Leadership, governance and responsibilities

Headteacher and senior leaders

- hold overall duty of care for the safety of the school community, including online safety;

- ensure appropriate leadership, resources, training, filtering, monitoring and reporting arrangements are in place;
- ensure serious allegations involving staff are managed through safeguarding and managing-allegations procedures;
- receive appropriate monitoring information and ensure actions arising from incidents are implemented.

Governing Body

- approves this policy and reviews its effectiveness;
- receives appropriate, anonymised information about online safety incidents, trends, education, training, filtering and monitoring;
- ensures safeguarding governance includes online safety and that a designated governor provides appropriate challenge and oversight.

Designated Safeguarding Person / Online Safety Lead

- takes day-to-day responsibility for online safeguarding, or works closely with the nominated Online Safety Lead where these roles are separate;
- ensures staff understand how to report online safety concerns immediately;
- coordinates responses to online safeguarding concerns and ensures appropriate records are maintained;
- liaises with senior leaders, pastoral staff, technical staff, the local authority, police and other agencies as required;
- supports staff, learner, parent/carer and governor training and awareness;
- reviews patterns and trends and recommends changes to policy, curriculum or technical controls.

Curriculum and pastoral leaders

Curriculum and pastoral leaders will ensure that online safety and digital resilience are planned progressively through the curriculum, the Digital Competence Framework, Health and Well-being/PSE provision, assemblies, tutor time and relevant national initiatives.

Teaching and support staff

- understand that online safety is a core safeguarding responsibility;
- follow this policy, the Staff Acceptable Use Agreement and school safeguarding procedures;
- use official school systems for professional communication with learners and parents/carers;
- supervise the use of technology appropriately and model safe, responsible and professional behaviour;
- report concerns, suspected misuse or harmful content immediately through the school's agreed safeguarding route;
- do not investigate safeguarding concerns themselves or retain/share illegal imagery.

Technical staff / managed service provider

- maintain secure infrastructure, accounts, permissions, filtering and monitoring systems;
- apply technical controls consistently and maintain appropriate logs;
- report significant misuse, attempted bypasses, cyber-security incidents or safeguarding alerts promptly;

- support authorised investigations without compromising evidence or safeguarding procedures.

5. Learners, parents/carers and community users

Learners

- use school technology in accordance with the Learner Acceptable Use Agreement;
- keep passwords and accounts secure and never use another person's credentials;
- report harmful, worrying, abusive or inappropriate online content or contact;
- treat others with respect online and do not create, request, share or forward harmful, abusive or sexual content;
- respect copyright, privacy and personal data;
- understand that school expectations may apply to online behaviour outside school when it affects members of the school community.

Parents and carers

Parents and carers are important partners in online safety. The school will provide information and guidance through appropriate communication channels and will encourage families to reinforce safe and responsible use of technology at home. Parents/carers should report concerns to the school promptly and support school expectations regarding personal devices and online conduct.

Visitors, volunteers and community users

Any person given access to school digital systems must follow the relevant Acceptable Use Agreement and school safeguarding expectations. Access will be proportionate to role and removed when no longer required.

6. Acceptable use of technology

Area	Darland expectation
School accounts and passwords	Use only your own account. Keep credentials secure. Do not share passwords or attempt to access another user's account.
Internet access	Use for learning, school business and authorised activity. Do not bypass filtering or monitoring.
Communication	Use school-approved systems. Communication must be professional, respectful and appropriate.
Images and recording	Only take, store or share images/recordings when authorised and for a legitimate purpose.
Personal devices	Learners may bring mobile phones to school but they must be switched off and away during the school day in line with the Behaviour for Learning Policy, unless a specific authorised exception applies.
Social media	Do not use social media in a way that bullies, harasses, discriminates, breaches privacy, damages professional boundaries or brings the school community into disrepute.

Copyright and data	Respect copyright, licensing, confidentiality and data-protection requirements.
Cyber security	Do not install unauthorised software, introduce malware, probe systems, disrupt services or attempt to circumvent security controls.

7. Unacceptable and illegal use

The following are prohibited. This list is not exhaustive and the seriousness of an incident will determine the response.

Category	Examples	Typical response
Illegal / potentially criminal	Child sexual abuse material; grooming; threats of violence; hate crime; terrorism/extremism; fraud; weapons-related offences; serious harassment or stalking; cyber-crime.	Immediate safeguarding escalation; preserve evidence; police/local authority involvement as appropriate.
Safeguarding harm	Sexual harassment; sharing nudes/semi-nudes; coercive or abusive contact; online bullying; harmful challenges; content linked to self-harm or exploitation.	Safeguarding response, support for those affected, parents/carers informed where appropriate, behaviour response and external referral where required.
Security misuse	Password sharing; account misuse; bypassing filtering; unauthorised access; malware; deliberate disruption; data destruction.	Restrict access, technical investigation, behaviour/disciplinary action and external referral for serious/repeat cyber-crime.
Inappropriate use	Pornography; gambling; discriminatory material; unauthorised file sharing; copyright infringement; unauthorised recording; misuse of messaging/social media.	Proportionate behaviour/disciplinary response, education, parental contact and access restrictions as appropriate.

Important

Where illegal content or activity is suspected, staff must not conduct their own investigation. The concern must be reported immediately to the DSP/Headteacher and safeguarding procedures

followed. Devices and evidence should be secured and preserved without unnecessary viewing, copying or sharing.

8. Reporting and responding to incidents

All members of the school community should know how to report online safety concerns. Reports will be taken seriously and dealt with as soon as practicable. Learners should be able to report to any trusted adult; staff must then follow the school safeguarding route.

Step	Action
1. Recognise	Identify a concern, disclosure, alert, harmful content, suspected misuse or unsafe online behaviour.
2. Report	Report immediately to the DSP/appropriate safeguarding lead. Staff concerns involving the Headteacher are referred to the Chair of Governors and local authority in line with managing-allegations procedures.
3. Protect	Consider immediate safety and welfare. Do not ask leading questions. Do not forward or copy illegal images. Secure devices/evidence where appropriate.
4. Assess and refer	DSP/senior leaders determine safeguarding, behaviour, technical and external-agency actions. Police/local authority referrals are made where required.
5. Record	Record the incident using the school's safeguarding/incident recording system and retain relevant authorised technical evidence.
6. Support and follow up	Provide support, communicate with parents/carers where appropriate, apply proportionate sanctions/interventions, and review learning from the incident.

Darland may also use information from filtering and monitoring alerts, including Smoothwall alerts, SHARP communications, network activity and safeguarding records, to identify risk and patterns of concern.

9. Responding to learner misuse

Most incidents will be managed through the school's normal safeguarding and Behaviour for Learning procedures. Responses will be proportionate to the nature, intent, impact, age, vulnerability and history of the learner, and may include education and restorative work alongside sanctions.

Incident	Possible school actions
Accidental access to unsuitable material	Close/leave content, report to staff, record if needed, review filtering if appropriate.

Deliberate access to inappropriate content or bypassing filtering	Pastoral/SLT referral; parental contact; restriction of access; sanction; safeguarding review where necessary.
Account/password misuse or unauthorised network access	Secure account; technical review; sanction; parental contact; external advice/referral for serious or repeated cyber-security concerns.
Online bullying, harassment, discrimination or harmful messaging	Safeguarding and anti-bullying response; support for those affected; evidence preservation; parental contact; behaviour sanction; external referral where required.
Unauthorised images/recording or device misuse	Apply mobile/device and behaviour procedures; secure evidence where appropriate; safeguarding review if content is harmful or sexual.
Suspected illegal activity or serious harm	Immediate DSP/Headteacher escalation and referral to police/local authority as appropriate.

10. Responding to staff misuse

Concerns about staff use of technology must be reported immediately to the Headteacher. Where the concern relates to the Headteacher, it must be reported to the Chair of Governors and local authority in accordance with safeguarding and managing-allegations procedures. Responses may include restriction of access, investigation, HR advice, suspension, disciplinary action and referral to external agencies, depending on the circumstances.

11. Online safety education and digital resilience

Darland High School will provide a planned and coordinated approach to online safety education. Learners should develop the knowledge, skills and strategies needed to manage their online experiences safely and responsibly, protect their digital identity, recognise misinformation and manipulation, identify and mitigate risk, seek help and benefit positively from technology.

- Online safety will be embedded across relevant curriculum areas and the Digital Competence Framework.
- Health and Well-being/PSE, tutor time, assemblies and pastoral programmes will reinforce key messages.
- Teaching will be age-appropriate, inclusive and responsive to emerging risks without unnecessarily directing learners towards harmful content.
- Learner voice will be used, where appropriate, to understand trends and evaluate provision.
- Staff will receive appropriate updates and training; governors will receive safeguarding training and oversight information.
- Parents/carers will be signposted to reliable guidance and support.

12. Filtering and monitoring

The school will maintain filtering and monitoring arrangements appropriate to the age of learners, the school's safeguarding responsibilities and local authority requirements. Filtering and monitoring are safeguards, not substitutes for effective supervision, education and professional judgement.

- Filtering will seek to block illegal and inappropriate content while supporting legitimate teaching and learning.
- Monitoring alerts and logs will be reviewed by authorised staff and escalated where they indicate safeguarding or security concerns.
- Requests to change filtering will be authorised, recorded and reviewed appropriately.
- Attempts to bypass filtering or monitoring are prohibited and may result in sanctions or further investigation.
- Access to monitoring information will be restricted to those who need it for safeguarding, security or authorised investigation.

13. Technical security and cyber security

- Users must authenticate using their own credentials and follow password/MFA requirements where provided.
- Devices, systems and software must be maintained and updated by authorised personnel.
- Users must not install unauthorised software or connect unauthorised equipment that creates security risk.
- Personal or confidential data must be stored and transferred only through approved systems.
- Suspected phishing, malware, account compromise or data breach must be reported immediately.
- Backups, access controls, patching and recovery arrangements will be maintained in line with school/local authority requirements.

14. Mobile technologies and personal devices

Darland High School recognises that mobile technology can support learning but can also create distraction, safeguarding, privacy and behaviour risks. The school's Behaviour for Learning Policy therefore governs learner use of mobile phones and personal devices.

Darland learner expectation

Mobile phones must be switched off and away once learners are in school. They must not be used during lessons, social times or movement around school unless a member of staff has given a specific authorised exception for a defined purpose. Unauthorised use will be addressed through the school behaviour system.

The school may introduce or operate arrangements requiring devices to be handed in or securely stored during the school day where this is considered necessary. Any change to the operational arrangement will be communicated clearly to students, staff and parents/carers.

Students bring mobile phones and other personal electronic devices onto the school site at their own risk. The school cannot accept responsibility for loss or damage except where responsibility arises under law.

OR

Darland learner expectation

Learners' mobile phones and other personal electronic devices must be handed in at the start of the school day and will be returned at the end of the day. Mobile phones and other electronic devices are therefore not permitted for use during the school day, including during lessons, social times and movement around the school site. Any unauthorised possession or use of a mobile phone or other electronic device during the school day will be addressed through the school behaviour system.

Staff use of personal devices must maintain professional boundaries, confidentiality and safeguarding. Personal devices must not be used as an informal channel for communicating with learners or parents/carers. Images or recordings of learners must only be made and stored using authorised arrangements.

15. Social media and online communication

- Professional communication with learners and parents/carers must use school-approved systems and accounts.
- Staff must maintain professional boundaries and must not use personal social media, personal email or private messaging for routine communication with learners.
- Users must not post confidential, defamatory, discriminatory, harassing or safeguarding-sensitive information.
- Only authorised staff may publish on official school websites or social media accounts.
- Online conduct outside school may be addressed where it affects safeguarding, staff professional standing, learners, or the reputation and orderly operation of the school.

16. Digital images, video and publishing

- Images and recordings must have a legitimate educational or school purpose and follow consent/privacy arrangements.
- Learners must not take images or recordings of others without permission.
- Content published by the school will be checked for safeguarding, data-protection, copyright and reputational considerations.
- Names and identifying information will not be combined with images where doing so creates unnecessary risk.

17. Data protection and confidentiality

Personal data must be handled lawfully, fairly, securely and only for legitimate school purposes. Users must follow the school's data-protection arrangements, use approved storage and communication systems, and report suspected loss, disclosure or compromise of personal data immediately.

18. Monitoring, evaluation and review

The policy will be reviewed at least annually and sooner where there are significant technological developments, new or emerging online harms, changes in statutory/national guidance, or serious incidents. The school will evaluate impact using appropriate evidence, which may include:

- safeguarding and online safety incident records;
- Smoothwall/filtering and monitoring alerts and trends;
- SHARP communications and learner reporting;
- network/security information and technical logs;
- learner, staff and parent/carers feedback;
- curriculum and training reviews;
- governor safeguarding oversight.

Review question	Evidence to consider
Are learners safer and more confident online?	Learner voice, incident trends, curriculum evidence, reporting confidence.
Are staff responding consistently?	Training, safeguarding records, staff feedback, incident reviews.
Are technical controls effective and proportionate?	Filtering/monitoring trends, bypass attempts, security incidents, change logs.
Are parents/carers appropriately informed?	Communications, engagement, feedback and support requests.

Appendix 1 - Learner Acceptable Use Agreement

I understand that school technology is provided to support learning and that I am responsible for using it safely and respectfully. I agree that:

- I will use only my own account and will keep my password secure.
- I will not try to bypass filtering, monitoring or security controls.
- I will not deliberately access, create, request, share or forward illegal, harmful, abusive, discriminatory, sexual or otherwise inappropriate content.
- I will treat others respectfully online and will not bully, harass, threaten or impersonate others.
- I will report anything online that worries, upsets or frightens me, or anything I think may put another person at risk.
- I will respect privacy, personal data, copyright and the work of others.
- I will only take or share images/recordings when I have permission and it is appropriate to do so.
- My mobile phone will be switched off and away in school unless a member of staff gives me a specific authorised exception.
- I understand that the school may monitor use of its systems and may take action if I misuse technology, including where online behaviour outside school affects the school community.

Learner name	
Signature / acknowledgement	
Date	

Appendix 2 - Staff and Volunteer Acceptable Use Agreement

- I will use school systems and devices professionally, lawfully and in accordance with safeguarding and data-protection requirements.
- I will use only authorised communication channels with learners and parents/carers and maintain professional boundaries.
- I will protect passwords, accounts, confidential information and personal data.
- I will not bypass filtering/monitoring, install unauthorised software or use systems in a way that creates security risk.
- I will immediately report safeguarding concerns, harmful content, security incidents, data breaches and suspected misuse through the correct school route.
- I will not investigate safeguarding concerns myself or copy/share illegal imagery.
- I will use images, recordings, cloud services and online publishing only in accordance with school procedures and permissions.
- I understand that school systems may be monitored and that misuse may be addressed through disciplinary, safeguarding or legal procedures.

Name	
Role	

Signature / acknowledgement	
Date	

Appendix 3 - Online Safety Incident Quick Guide

If you are concerned

REPORT IMMEDIATELY to the Designated Safeguarding Person / safeguarding team. If a child may be at immediate risk, follow emergency safeguarding procedures.

DO	DO NOT
Listen, reassure and record factual information.	Do not promise confidentiality.
Preserve evidence and secure devices if instructed.	Do not investigate the matter yourself.
Record websites(URLs)/usernames/times where safe and appropriate.	Do not repeatedly view harmful or illegal content.
Follow DSP/Headteacher instructions and external-agency advice.	Do not copy, print, forward or screenshot child sexual abuse imagery.
Keep information on a strict need-to-know basis.	Do not ask leading questions or contact alleged perpetrators yourself.

External support and referral

Depending on the nature of the concern, the school may seek advice or make referrals to the local authority safeguarding/ICT teams, police, CEOP, the Professionals Online Safety Helpline, Hwb online safety resources or other appropriate agencies. Emergency or criminal matters will be escalated without delay.

Appendix 4 - Policy adoption record

Action	Date / detail
Consultation with staff	
Learner voice / consultation	
Parent/carers consultation where appropriate	
Governor review	September 2026
Governing Body approval	September 2026
Published / communicated	October 2026
Next review	September 2027

