Greenfields School Internet Safety Policy 2025-2026

Implemented	By Whom	Last Review	By Whom	Next Review
June 2025	R.Hill	March 2026	R. Redman and C.Singh	March 2027

Document History (last 3 versions)			
Date of Issue	**Version No.**	**Person(s) responsible for change**	**Nature of Change**
17/06/24	1	J. Parry	Review and amendment
08/09/25	2	R. Redman	Review and amendment
03/10/25	3	Creslyn Singh	Review and amendment
12/03/26	4	Creslyn Singh	Reviewed

This policy also aligns with Welsh Government "Keeping Learners Safe" (2022), Hwb Online Safety Guidance, Wales Prevent Duty Guidance, and the Wales Safeguarding Procedures (2019).

Mission Statement

Preparing learners for the future by providing a sustainable outstanding educational experience where all learners realise pursue and achieve their full potential, enabling them to thrive as adults.

Aims

- To provide learners with quality Internet access as part of their learning experience across all curricular areas.
- To provide clear advice and guidance in order to ensure that all Internet users are aware of the risks and the benefits of using the Internet.
- To evaluate Internet information and to take care of their own safety and security.
- To raise educational standards and promote learner achievement.
- To work with other schools and the local authority to share good practice in order to improve this policy.

Online Safety at Greenfields reflects the expectations of Welsh Government's Digital Competence Framework values, without claiming delivery of the Curriculum for Wales framework.

We have a duty to provide learners with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.

Used safely Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the learners school experiences.

We acknowledge that the increased provision of the Internet in and out of school brings with it the need to ensure that learners are safe. We need to teach learners how to evaluate Internet information and to take care of their own safety and security.

E-Safety, which encompasses Internet technologies and electronic communications, will educate learners about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

Using the internet for online research is a valuable activity that learners need to understand as they prepare for adult life.

However, the learners attending Greenfields School can have histories of poor behaviour and some may have inappropriate usage prior to joining the school so please refer to individual learner risk assessments prior to using internet access to ensure correct measures of supervision are in place.

On occasions there may be a specific prohibition order concerning internet access applied to a young person by a court order. In this case, staff must, where necessary for the purposes of education, access the internet on behalf of the young person and relay any necessary information to them by printing out information for lessons.

Many Greenfields learners have social, emotional or trauma-related vulnerabilities which increase their risk online. Staff follow individual risk assessments and supervision plans to ensure safe use of devices and digital platforms.

Online activity relating to radicalisation, extremist content or concerning ideology will be escalated immediately to the DSP and Newport Prevent team and/or the LA the learners placement is funded by.

Creslyn Singh and Rhys Redman (SLT) are the responsible people for ensuring that this policy is implemented and embedded as a CEOP's Ambassador and ensures training is provided for staff & learners.

Safe usage
The school Internet access will:
- be designed for learners use.
- Under no circumstances should learners have unsupervised access to the internet.
- include school filtering configuration
- provide filtering which is reviewed annually and improved if necessary;
- include filtering appropriate to the age of learners;
- have virus protection installed which will be updated regularly;
- be constantly monitored

– E-Safety Lead / CEOP Ambassador – Rhys Redman
– Deputy E-Safety Lead – Creslyn Singh
– DSP / Safeguarding Lead – Rhys Redman (for exploitation concerns)
–Proprietor – rob Mcconomy (oversight of online safety governance)

Authorising Internet Access
- Before using any school ICT resource, all learners and staff must read and sign the 'Acceptable ICT Use Agreement'.
- All learners and school personnel will have Internet access monitored
- Any learners with high risks will have risk assessments in place & strategies put in place to educate learners so IT can be used.

Inappropriate Material
- Any inappropriate websites or material found by learners or school personnel will be reported to the e-Safety Coordinator who in turn will report to the Internet Service Provider to be added to Fortitude to block future access.
- Any online risk, exploitation concern, or harmful digital behaviour is treated as a safeguarding matter and escalated immediately using Wales Safeguarding Procedures (2019) and Greenfields' Child Protection Policy.

Curriculum
- School will promote safe usage through workshops, displays & thematic days.
- Learners will use ICT across the curriculum, skills challenge writing cv, creating PowerPoints for discussions/presentations in subjects, using word to type, use of interactive boards in subjects etc.

Digital Images, Video & Recordings
– Images or recordings of learners must only be taken on school devices.
– No personal devices may be used.
– All images must follow GDPR (UK) and school consents.
– Images must not be stored on personal cloud systems.

Internet System Security
- Fortitude
- Everyone must be aware that under the Computer Misuse Act 1990 the use of computer systems without permission or for inappropriate use could constitute a criminal offence.
- Filtering and monitoring arrangements meet Welsh Government expectations and are reviewed by CAE (Our It System). Hwb digital standards inform filtering decisions and acceptable use.

Complaints of Internet Misuse
- The Head teacher/Deputy will deal with all complaints of Internet misuse by school personnel or learners.
- Parents/Carers/Carers will be informed if their child has misused the Internet.

- Cyberbullying incidents are managed in line with the Greenfields Anti-Bullying Policy and recorded on BehaviourWatch.

Social Networking and Personal Publishing

Learners will not be allowed access:

- to social networking sites except those that are part of an educational network or approved Learning Platform;
- to newsgroups unless an identified need has been approved

Registering for most social networking sites requires each user to enter their date of birth and other personal details such as an email address, name, etc. Most major social media platforms have a minimum age of 13 in line with international COPPA standards. Learners must not access social media on school devices under any circumstances.

Please find a list of pages to report abuse for the social network providers named above:

- Facebook – https://www.facebook.com/help/359033794168099/
- Twitter – https://support.twitter.com/articles/15794-online-abuse
- Pinterest – https://help.pinterest.com/en-gb/article/report-harassment-and-cyberbullying
- Google Plus+ - https://support.google.com/plus/answer/2463131?hl=en
- Tumblr - https://www.tumblr.com/policy/en/community
- Instagram - https://help.instagram.com/165828726894770/
- Flickr - https://www.flickr.com/report_abuse.gne
- Snapchat - https://support.snapchat.com/co/harassment

E-mail

Learners must:

- report receiving any offensive e-mails;
- not divulge their or others personal details;
- not arrange to meet anyone via the e-mail;
- not take part in sending chain letters

If the bullying is persistent it's possible to block a particular senders e-mail address. An alternative is for the person being bullied to change their email addresses. Your email provider will have information in the "Help" or "Support" section of their website and also information on how to create a new account. School will also address the matter in line with our bullying policy.

Details for reporting offensive content from some of the most popular email providers include:

- Outlook.com (Hotmail / Office 365) - https://support.microsoft.com/en-us/office/phishing-and-suspicious-behaviour-0d882ea5-eedc-4bed-aebc-079ffa1105a3 or email abuse@outlook.com
- GMail - https://support.google.com/mail/contact/abuse
- Yahoo! Mail - https://help.yahoo.com/kb/SLN3403.html
- mac.com / iCloud - To report suspicious emails that you have received in your iCloud.com, me.com or mac.com inbox, please send them to abuse@icloud.com.

Instant Messages (IM) have become integrated to other popular services, especially social networking. For integrated and stand-alone IM providers it is usually possible to block messages from offensive users. For stand-alone IM services users are at liberty to change Instant Messenger IDs so that a bully is not able to contact their victim any more. Many providers have information on their website about how to do this. In addition, the Instant Messenger provider can investigate and shut down any accounts that have been misused and clearly break their terms of service. The best evidence for submitting to your IM provider is archived or recorded conversations and many IM providers allow their users to record all messages.

Registering for many IM applications requires users to enter in their date of birth as well as other standard details such as an email address, name, etc. Please find below the legal age requirement for the most popular IM applications:

- Skype – No age restrictions;
- Facebook Messenger – 13 years and older;
- SnapChat - 13 years and older;
- WhatsApp – 16 years and older;
- Yahoo Messenger - 18 years and older to use the chat facility;
- AIM (AOL Instant Messenger) – 13 years and older.

The current mechanisms to report IM abuse to these providers include:

- Skype - https://support.skype.com/en/faq/FA34447/what-should-i-do-if-i-see-abusive-behavioron-skype
- Facebook Messenger - https://www.facebook.com/help/messenger-app/1642061529351598/
- SnapChat - email safety@snapchat.com or click “Support” on the app;
- WhatsApp – Block offensive messages in the WhatsApp app;

Raising Awareness of this Policy

We will raise awareness of this policy via:

- the School Handbook/Prospectus
- the school website
- the Staff Handbook
- meetings with Parents/Carers such as introductory, transition, parent/carer-teacher consultations and periodic curriculum workshops
- school events
- meetings with school personnel
- communications with home such as weekly newsletters and of end of half term newsletters
- reports such annual report to Parents/Carers and Head teacher reports to the Proprietor/Nominated person
- information displays in the main school entrance

Training

All school personnel:

- have equal chances of training, career development and promotion
- receive training on induction which specifically covers:
  - All aspects of this policy
  - Safeguarding & Child Protection
  - CEOPS
  - ICT – Staff will sign Acceptable Internet Use Agreement
  - GDPR Data Protection
  - Anti-bullying
  - Mobile Phone Safety
  - Photographic & Video Images
  - Internet Social Networking Websites are age restricted & not to be accessed during school day
- receive periodic training so that they are kept up to date with new information
- receive equal opportunities training on induction in order to improve their understanding of the Equality Act and its implications.

The following documentation is also related to this policy:

- Keeping Learners Safe (WG 2022)
- Wales Safeguarding Procedures (2019)

- Online Safety in Wales: Hwb Digital Safety
- Safer Working Practice for Adults who Work with Children (Education Workforce Council Wales)
- Prevent Duty (Wales)
- Education Workforce Council (EWC) Code of Professional Conduct.

Staff must not:
– communicate with learners via social media
– accept learners as followers or contacts
– store learner data on personal devices

Mobile Devices
– Learners' personal devices are handed in on arrival
– Staff mobile phones must not be used during teaching time
– Recording or photographing learners on personal devices is prohibited
– Phones are stored securely

Monitoring the Effectiveness of the Policy
The practical application of this policy will be reviewed annually or when the need arises by the coordinator, the Head teacher.

Headteacher:	Creslyn Singh	**Date:**	22nd October 2025
Proprietor:	Rob McConomy	**Date:**	22nd October 2025

APPENDIX A – Kept in staff personnel files

Acceptable ICT Use Agreement

I understand that the school Internet facility is for the good of my professional development, for the development of this school and must be used only for educational purposes.

I realise that I have a personal responsibility to abide by the set rules and regulations when using the Internet and I am aware of the consequences if I breach them. I am aware that by beaching the rules and regulations it may lead to:

- withdrawal of my user access
- the monitoring of how I use the Internet
- disciplinary action
- criminal prosecution

I will report immediately to the E-Safety Coordinator any accidental access to inappropriate material or websites that I may have.

I will log on to the Internet by using my password, which will be changed every half term, or if I think someone knows it. When using the school's Internet I will not:

- use the Internet in such a way that it will bring the school into disrepute
- use inappropriate or illegal websites
- use the internet for personal usage during contractual work hours
- download inappropriate material or unapproved software
- disrupt the time of other Internet users by misusing the Internet
- use inappropriate language
- use language that may provoke hatred against any ethnic, religious or other minority group
- produce, send out, exhibit or publish material that will cause offence to anyone
- divulge any personal information about myself, any other user or that of learners
- divulge my login credentials or passwords to anyone
- use the login credentials or passwords of any other user
- use a computer that is logged on by another user
- use any social networking site
- transfer the images of learners without prior permission of the head teacher and from guardians
- use email for private use but only for educational purposes
- compromise the Data Protection Act or the law of copyright in any way

I agree to abide by this agreement.

Employee Name:		**Head teacher Name:**	
Employee Signature:		**Head teacher Signature:**	
Date:		**Date:**	