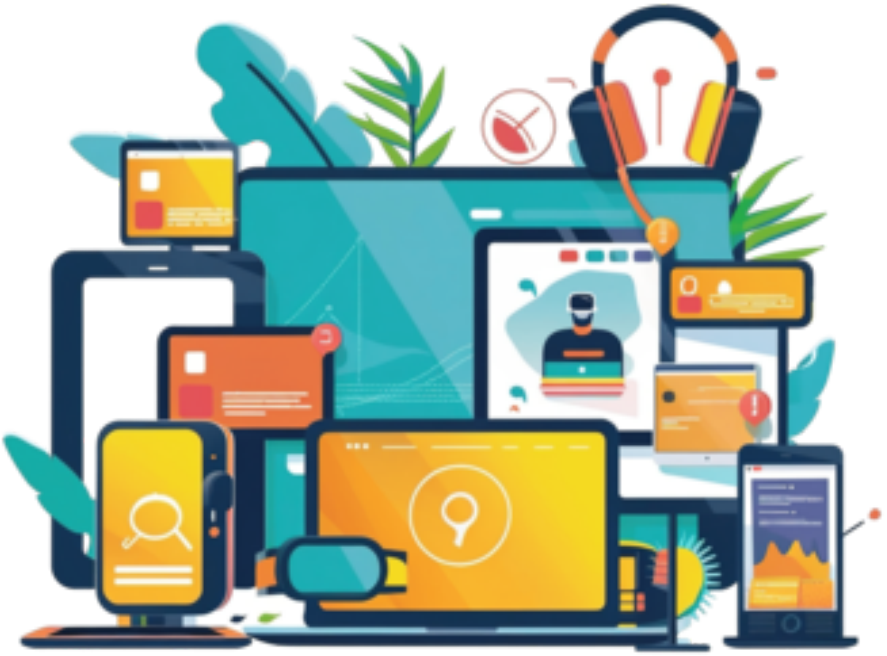
Rhydypenau Primary School

"Aiming High"



E-Safety Policy

Development, Monitoring & Review of this Policy

The Headteacher monitors the effectiveness of this policy on a regular basis. They also report to the Governing Body on the effectiveness of the policy and, if necessary, make recommendations for further improvements.

Schedule for Development, Monitoring & Review

This policy was agreed by teachers:	
This policy was agreed and adopted by the Governing Body:	
The implementation of this policy will be reviewed by:	
This policy will be reviewed:	Every 2 two years
This policy was last reviewed:	September 2025
This policy is due to be reviewed:	September 2027
Chair of Governors' Signature:	
Headteacher's Signature:	

Introduction

The purpose of this E-Safety Policy is to set out a clear framework that ensures all members of the school community are safe, responsible, and respectful users of digital technologies. At Rhydypenau Primary School, we recognise that access to digital tools and the internet is an important part of learning and personal development. However, we are equally aware of the risks associated with online activity and the need to protect pupils from potential harm.

Aims of this policy:

- To safeguard pupils, staff, and the wider school community from online risks, including cyberbullying, exploitation, and inappropriate or harmful content.
- To ensure that pupils develop the knowledge, skills, and confidence to use digital technologies safely and responsibly, both inside and outside of school.
- To provide clear expectations and guidelines around the use of mobile phones, smart devices, and school ICT systems.
- To ensure that staff, parents, and carers are equipped with the information and support they need to promote safe digital practices.
- To establish a culture of shared responsibility for e-safety across the whole school community.

This policy has been written in line with Welsh Government digital standards, Cardiff Local Authority guidance, and the principles of the United Nations Convention on the Rights of the Child (UNCRC). It will be reviewed on a 2 yearly cycle to ensure that it remains up to date with new technologies, emerging risks, and updated legislation.

Rights Respecting Approaches

At Rhydypenau Primary School, we are committed to fostering an environment that values and upholds the rights of every child. We are proud to introduce a rights-respecting approach into our policies, recognising the inherent dignity and worth of each learner, Rhydypenau Primary School aims to align our practices with the principles of the United Nations Convention on the Rights of the Child (UNCRC) to nurture their strong sense of belonging, and instil a deep understanding of the rights and responsibilities to all stakeholders.

Article 3 Best Interests of the Child

When adults make decisions, they should think about how their decisions will affect children. All adults should do what is best for children. Governments should make sure children are protected and looked after by their parents, or by other people when this is needed. Governments should make sure that people and places responsible for looking after children are doing a good job.

Article 16 Protection of Privacy

Every child has the right to privacy. The law must protect children's privacy, family, home, communications and reputation (or good name) from any attack.

Article 17 Access to Information

Children have the right to get information from the Internet, radio, television, newspapers, books and other sources. Adults should make sure the information they are getting is not harmful. Governments should encourage the media to share information from lots of different sources, in languages that all children can understand.

Article 18 Responsibility of Parents
Parents are the main people responsible for bringing up a child. When the child does not have any parents, another adult will have this responsibility and they are called a "guardian". Parents and guardians should always consider what is best for that child. Governments should help them. Where a child has both parents, both of them should be responsible for bringing up the child.

Article 28 Access to Education
Every child has the right to an education. Primary education should be free. Secondary and higher education should be available to every child. Children should be encouraged to go to school to the highest level possible. Discipline in schools should respect children's rights and never use violence.

Article 29 Aims of Education
Children's education should help them fully develop their personalities, talents and abilities. It should teach them to understand their own rights, and to respect other people's rights, cultures and differences. It should help them to live peacefully and protect the environment.

Scope of the Policy

This policy applies to all members of the school (including staff, pupils, volunteers, parents, carers, visitors, community users) who have access to, and are users of school ICT systems, both in and out of the school.

The Education & Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of school, but is linked to membership of the school. The Education Act 2011 increased these powers with regard to the searching for and of, electronic devices and the deletion of data. In the case of both Acts, action can only be taken over issues covered by the published Behaviour Policy.

The school 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 e-safety behaviour that takes place outside of school.

Roles & Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Governors
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors who will receive regular information about e-safety incidents and monitoring reports.

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs

- regular monitoring of filtering/change control logs
- reporting to relevant Governors meetings

Headteacher

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co ordinator.

The Headteacher and (at least) one other member of the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see flow chart on dealing with e-safety incidents – included in a later section – 'Responding to Incidents of Misuse' and relevant Local Authority HR/other relevant body disciplinary procedures).

The Headteacher is responsible for ensuring the E-Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant. ⇒ The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the E-Safety.

School Digital Leader

The school digital leader is responsible for taking day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies & documents. They are responsible for ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place and provide training and advice for staff, or signpost staff to relevant guidance.

The school digital will liaise with the Local Authority and relevant bodies and with Schools Information Technology Services. They will attend relevant meetings of Governors and report issues and updates regularly to the Senior Leadership Team.

Technical Staff and Support Provided by Local Authority

IT support staff are responsible for ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack and ensure that the school meets required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.

Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed regularly. The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

They keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. The use of the network/internet/virtual learning environment/remote access/email is regularly monitored

in order that any misuse/attempted misuse can be reported to the Headteacher/E-Safety Co-ordinator/ICT Co-ordinator for investigation/action/sanction.

Teaching & Support Staff

Teaching and support staff are responsible for ensuring that they have an up to date awareness of e-safety matters and of the current school E-Safety Policy and practices and they have read and understand the ICT Acceptable Use Policy (Appendix A) and the Mobile Device Acceptable Use Policy (MAUP Appendix B).

Staff must report any suspected misuse or problem to the Headteacher or Digital Lead. Any matters of suspected misuse or problem must be reported through My Concern.

All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems.

E-safety issues are embedded in all aspects of the curriculum and other activities and should be taught regularly to students/pupils to build their awareness of correct device usage.
Staff are responsible for enforcing the acceptable usage policy within their own classrooms and understand and follow the e-safety and acceptable use policies. They monitor the use of iPads and laptops in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

In lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

In the event of technical issues, it is the teacher's or support staff's responsibility to report this initially to the digital lead. Should further assistance be required, staff should log a call using the local authority portal at https://ies.cardiff.gov.uk/portal/

Responding to Incidents involving staff		
Incidents	**Action**	**Sanction**
Deliberately accessing or trying to access material that could be considered illegal (see list below on unsuitable/ inappropriate activities).	• Refer to the headteacher • Refer to local authority Refer to police	Outcome determined by LA/Police
Inappropriate personal use of the internet/social media/personal email.	• Refer to digital leader • Refer to headteacher	Warning or disciplinary action
Unauthorised downloading or uploading of files.	• Refer to digital leader • Refer to headteacher	Warning or disciplinary action
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	• Refer to digital leader • Refer to headteacher	Warning or disciplinary action
Careless use of personal data e.g. holding or transferring data in an insecure manner.	• Refer to digital leader • Refer to headteacher	Warning or disciplinary action

Deliberate actions to breach data protection of network security rules.	• Refer to digital leader • Refer to headteacher	Warning or disciplinary action
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.	• Refer to digital leader • Refer to headteacher	Warning or disciplinary action
Sending an email/text/message that is regarded as offensive, harassment or of a bullying nature.	• Refer to digital leader • Refer to headteacher • Refer to local authority • Refer to police	Suspension and/or disciplinary action
Using personal email/social networking/instant messaging/text messaging to carry out digital communications with pupils.	• Refer to digital leader • Refer to headteacher	Warning or disciplinary action
Actions which could compromise the staff member's professional standing.	• Refer to digital leader • Refer to headteacher	Warning or disciplinary action
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.	• Refer to digital leader • Refer to headteacher	Warning or disciplinary action
Using proxy sites or other means to subvert the school's filtering system.	• Refer to digital leader • Refer to headteacher • Refer to local authority • Refer to police	Warning or disciplinary action
Accidentally accessing offensive or pornographic material and failing to report the incident.	• Refer to digital leader • Refer to headteacher	Warning or disciplinary action
Deliberately accessing or trying to access offensive or pornographic material.	• Refer to digital leader • Refer to headteacher • Refer to local authority • Refer to police	Warning or disciplinary action
Breaching copyright or licensing regulations.	• Refer to digital leader • Refer to headteacher	Warning or disciplinary action
Continued infringements of the above, following previous warnings or sanctions.	• Refer to digital leader • Refer to headteacher • Refer to local authority	Warning, Suspension and/or disciplinary action

Learners

Learners are responsible for using the school digital technology systems in accordance with the Pupil Information Communication & Technology Acceptable Use Policy (Appendix C). They will have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations and be taught about this through the curriculum.

Learners need to understand the importance of reporting abuse, misuse or access to inappropriate materials and must know how to do so.

Learners will be expected to know and understand policies on the use of mobile devices and digital cameras, and understand the policies on the taking/use of images and on cyber-bullying.

Learners must understand the importance of adopting good e-safety practice when using digital technologies out of school and must realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Learner Passwords

Initially, ie when they come into reception, pupil passwords will be set as follows:

Password: pupils initials in capital letters - rps - year they leave school - ! *So for Jane Ali who leaves school in 2029 the password will be:* **JArps29!**
This will enable all pupils to have individual passwords whilst also enabling class teachers/ other adults to be able to log in for them if there are any issues.

Use of Artificial Intelligence (AI) tools

Some external AI platforms (e.g. ChatGPT, Bard and similar services) set minimum age restrictions in their own terms and conditions, often age 13 or higher. The school does not rely solely on those limits but instead sets its own expectations:

- Pupils may only access generative AI tools for learning when this has been explicitly authorised by a teacher and under supervision.
- No personal, sensitive or identifiable data must ever be entered into external AI platforms.
- Pupils will be taught about the risks of bias, inaccuracy and inappropriate content from AI systems.
- Any suspected misuse or safeguarding concern related to AI is reported through My Concern and handled by the Designated Safeguarding Lead (DSL).

Remote learning and live online lessons

When remote teaching takes place, the following safeguards are applied:

- Staff use only school-approved platforms with secure logins.
- Lessons are conducted in a professional setting, with staff ensuring an appropriate background.
- One-to-one sessions are avoided unless specifically authorised by the Headteacher /DSP; where these occur, they must be recorded or supervised.
- Pupils and parents are reminded not to record or share live lessons without permission.
- Any safeguarding disclosures made during online sessions are reported immediately via My Concern.

School Actions & Sanctions

It is likely that the school will need to deal with incidents that involve inappropriate misuse of devices. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Incidents involving learners		
Incidents	**Action**	**Sanction**
Deliberately accessing or trying to access material that could be considered illegal	• DSP's informed & My Concern completed. • Next steps decided by HT/DHT and MASH • Consider police contact	To be agreed upon with the headteacher/deputy headteacher
Unauthorised use of non-educational sites during lessons.	• My Concern incident • Address with learner • Notify parents • Consider follow up learning opportunities	2 weeks restriction of school devices
Unauthorised use of mobile phone/digital camera/ other mobile device including smart devices	• My Concern incident • Address with learner • Notify parents • Consider follow up learning opportunities	Liaise with parents and consider restriction of device in school
Unauthorised use of social media/messaging apps/ personal email.	• My Concern incident • Address with learner • Notify parents • Teacher to plan further lesson on internet & device safety	2 weeks restriction of school devices if an incident is undertaken on school devices.
Unauthorised downloading or uploading of files.	• My Concern incident • Address with learner • Notify parents • Teacher to plan further lesson on internet & device safety	Class teacher to use discretion whether to restrict use of device for a duration (Recommended 1 or 2 days)
Sharing username and passwords.	• Address with learner • Notify parents due to personal data breach • User to consider changing password. • Teacher to plan further lessons on private information	None
Attempting to access or accessing the school network, using the account of a member of staff.	• My Concern incident • Address with learner • Notify parents • Teacher to plan further lesson on internet & device safety • Member of staff to secure account	Monitor ongoing usage of the devices
Attempting to access or accessing the school network, using another pupil's account.	• Address with learner • Notify parents due to personal data breach • User to consider changing password. • Teacher to plan further lessons on private information	2 Weeks restriction of school devices
Corrupting or destroying the data of other users.	• Address with learner • Notify parents • Notify Schools IT to try to retrieve missing data • Teacher to plan further lessons on private information	

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.	• My Concern incident • Initiate Anti-Bullying/ Anti-Racism policy • Address with learner • Notify parents • Teacher to plan further lesson on internet & device safety • Member of staff to secure account	
Continued infringements of the above, following previous warnings or sanctions.	• My Concern incident • Initiate Anti-Bullying/ Anti-Racism policy • Address with learner • Notify parents • Teacher to plan further lesson on internet & device safety • Member of staff to secure account	Consider further sanctions in line with the positive relationships policy
Action which could bring the school into disrepute or breach the integrity of the ethos of the school.	• My Concern incident • Address with learner • Notify parents • Consider follow up learning opportunities	Teacher discretion after consultation with Phase lead/HT/DHT
Using proxy sites or other means to subvert the school's filtering system.	• My Concern • Contact Schools IT service for advice • Notify Parents	2 Weeks restrictions of school devices
Accidentally accessing offensive or pornographic material and failing to report the incident.	• My Concern incident • Report to DSP • Discuss with learner and provide additional support where required • Notify parents • Consider follow up learning opportunities • Continue to check in with learner (wellbeing)	None
Deliberately accessing or trying to access offensive or pornographic material.	• DSP's informed & My Concern completed. • Next steps decided by HT/DHT and MASH • Consider police contact	2 Weeks restriction of school devices
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	• Discuss with learner • Provide additional learning opportunities about copyright and Data protection • Inform GDPR officer if it infringes up GDPR regulations • Notify affects individuals	Warning
Bypassing security controls in other ways: Attempting to disable antivirus, firewalls, monitoring software, or device management settings.	• My Concern • Contact Schools IT service for advice • Notify Parents	Warning
Use of unauthorised storage or transfer methods: Saving or transferring data via unapproved cloud services, file-sharing platforms, or peer-to-peer apps.	• My Concern • Contact Schools IT service for advice • Notify Parents • Remove files from unauthorised device • Teacher to plan follow	Teacher discretion

	lessons about file sharing	
Inappropriate use of cameras or recording features Taking or sharing images, videos, or audio recordings without consent, including covert recordings.	• My Concern incident • Address with learner • Notify parents • Consider follow up learning opportunities	2 Weeks Restriction of school devices
Impersonation or identity misuse: Logging into devices, platforms, or online services under a false identity or pretending to be someone else online.	• My Concern incident • Address with learner • Notify parents • Consider follow up learning opportunities	Teacher discretion. (Depending the circumstances i.e. if on school devices - 2 weeks restrictions applies)
Circumventing exam/assessment rules: Using devices to cheat, share answers, or access unauthorised information during tests.	• My Concern incident • Address with learner • Notify parents • Consider follow up learning opportunities	2 Weeks Restriction of school devices
Gaming misuse: Playing online or offline games during school hours without authorisation.	• My Concern incident • Address with learner • Notify parents • Consider follow up learning opportunities • Consider blocking websites if deemed inappropriate for school use	2 Weeks Restriction of school devices
Location and tracking misuse: Sharing or broadcasting live location data, or enabling location tracking that could compromise safety.	• My Concern incident • Address with learner • Notify schools IT if on school device to disable open location sharing • Notify parents who may need to disable sharing if on personal devices • Consider follow up learning opportunities	None
Use of AirDrop/Bluetooth/Nearby Share: Sending or receiving files, messages, or inappropriate content using short-range file transfer tools.	• My Concern incident • Address with learner • Notify schools IT if on school device to disable open location sharing • Notify parents who may need to disable sharing if on personal devices • Consider follow up learning opportunities	Consider restriction on school devices (Discretion of the teacher and SLT)
Streaming or bandwidth misuse: Excessive streaming, downloading, or uploading that impacts the school's network performance.	• Address with learner • Notify schools IT if deemed necessary	None
Digital plagiarism or academic dishonesty: Copying content directly from the internet or AI tools and presenting it as one's own work without attribution.	• My Concern incident • Address with learner • Notify parents • Consider follow up learning opportunities	Warning
Inappropriate AI use: Using generative AI or chatbots in ways that breach academic integrity, privacy, or safeguarding rules	• My Concern incident • Address with learner • If safeguarding - notify DSP's • Notify parents • Consider follow up learning opportunities	Consider restriction on school devices (Discretion of the teacher and SLT)

Parents & Carers

Parents/carers play a crucial role in ensuring their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to support parents/carers to understand these issues through parent evenings, meetings, newsletters, letters, websites and information about national or local e-safety campaigns. Parents/carers will be encouraged to support the school in promoting good e-safety practice and to ***follow guidelines on the appropriate use of digital and video images taken at school events.***

Community Users (e.g. Midday Supervisors, Supply Teachers, Parent Helpers etc.)

Community Users who access school systems/websites as part of the wider school provision will be expected to sign the Community User Acceptable Use Policy (CUAUP Appendix D) before being provided with access to the school systems.

Learners Using Personal Devices

Year 5 and below

- Pupils in Year 5 and below are **not permitted** to bring mobile phones into school under any circumstances.
- Other smart devices (e.g. smart watches, or any wearable or portable device with communication or internet capability) are also **not permitted** if those communication features are enabled.
- If such a device is seen, it will be confiscated and returned only to a parent or guardian, in line with the school's behaviour policy.

Year 6

- Pupils in Year 6 **may** bring mobile phones and other smart devices with communication capabilities into school.
- However, these devices must be handed in *at the beginning of the school day* and be **locked away securely** until the end of the day. Pupils are **not permitted** to access or use them during school hours.
- Smart devices with communication features are treated the same way—they may be brought in, but must be locked away securely for the day.
- Unauthorized use (i.e. accessing or using during the day) will be dealt with under the behaviour policy / safeguarding procedures.

Other Key Points

- Any devices brought for educational purposes may be exempted, but must be used under direct supervision of staff and in accordance with the school's digital / device-use guidelines.
- The school will ensure that parents/carers are informed of these expectations in advance.

Use of Digital Images & Videos

When using digital and video images, staff, parents/carers, and volunteers must follow the school's safeguarding and data protection responsibilities. This section reflects UK GDPR, the Data Protection Act 2018, and current Welsh Government guidance. The school's lawful basis for using photographs and video is normally **'public task'** under UK GDPR, as part of its role in providing education. Consent may be sought for additional uses (such as promotional materials), but parental opt-out or withdrawal requests are always respected.

Staff should:

- Inform and educate pupils about the risks associated with the taking, using, sharing, publication, and distribution of images. This includes highlighting the risks of publishing personal images on the internet (e.g. social media platforms).
- Ensure that all images and recordings taken for educational purposes are relevant, appropriate, and respectful of pupils' dignity.
- Only use school-owned equipment to capture digital images or videos for educational purposes. Personal devices must not be used except under explicit authorisation by the Headteacher, and only if the images are transferred immediately to school systems and deleted from the personal device.
- Take care to ensure pupils are appropriately dressed and not engaged in activities that could bring individuals or the school into disrepute.
- Follow school safeguarding policies regarding the use, storage, and deletion of digital media. Images containing personal or sensitive data must be stored securely on school systems, with access restricted to authorised staff. They are retained in line with the school's **Data Retention Policy** (e.g. images used for publicity are normally reviewed annually; images in records are retained in line with pupil file retention periods) and then securely deleted.

Parents/Carers:

- Parents/carers are welcome to take videos and digital images of their own children at school events for personal and family use only. Such use is exempt from data protection legislation, but images must not be shared publicly on social media, or in any way that identifies other children or staff without consent.
- Parents/carers must avoid naming children or staff in online posts linked to images/videos taken at school events.

Publication of Images:

- Photographs or videos published on the school website, newsletters, or official social media platforms will be selected carefully and comply with national good practice guidance.
- Pupils' full names will not be published alongside photographs. Images will not be tagged with specific locations until after an event has concluded.
- Written parental/carer consent will always be obtained before any pupil's image or work is published by the school. Pupils without written consent will not appear in publicly available media. **Parents/carers may withdraw consent at any time by contacting the school office or the Data Protection Officer (DPO). The school will respect withdrawals immediately and ensure that images are removed where practicable.**
- Pupils must not take, use, share, publish, or distribute images of others without permission.
- Pupils' work can only be published with permission from both the pupil and their

parent/carer.

Key Principle:

All use of digital and video images must prioritise the safeguarding, privacy, and dignity of pupils and comply with the school's Data Protection and Safeguarding Policies.

Data Protection

Personal data will be recorded, processed, transferred, and made available in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. These laws require that personal data must be:

- Processed lawfully, fairly, and transparently.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Stored only for as long as necessary.
- Processed in a manner that ensures appropriate security.
- Processed in accordance with the rights of the data subject.

The school must ensure that:

- It holds the minimum personal data necessary to perform its functions and does not keep it for longer than necessary.
- All reasonable steps are taken to ensure personal data is accurate and up to date; inaccuracies will be corrected without delay.
- All personal data is obtained and processed fairly, transparently, and in line with the school's Privacy Notice.
- A Data Protection Policy is in place and is reviewed regularly.
- The school is registered with the Information Commissioner's Office (ICO) as a Data Controller.
- A designated Data Protection Officer (DPO) is appointed, alongside Senior Information Risk Owner (SIRO) and Information Asset Owners (IAOs).
- Regular risk assessments are undertaken to manage and mitigate data protection risks.
- Clear and understood arrangements are in place for the security, storage, retention, and transfer of personal data.
- Data subjects' rights (including the right of access, rectification, erasure, restriction, and portability) are respected and supported through clear procedures.
- Policies and routines are in place for the secure deletion and disposal of data.
- There is a clear procedure for reporting, logging, managing, and recovering from data breaches or information risk incidents. **The DPO must be informed of suspected breaches within 24 hours, and where a breach is notifiable, the ICO will be informed within 72 hours.**
- Any use of cloud storage or cloud computing services complies with ICO requirements and UK GDPR safeguards.

Staff must ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss, misuse, or unauthorised access.
- Only use personal data on secure, password-protected devices and ensure they are

logged off or locked when not in use.

- Avoid the use of removable media (such as USB drives) unless absolutely necessary and authorised. Where used, devices must be encrypted, password protected, and compliant with the school's ICT Security Policy.
- Ensure that portable devices contain appropriate antivirus and malware protection.
- Securely delete personal data from portable devices once it has been transferred or is no longer required, in accordance with the school's Data Retention Policy.

Key Principle:

All personal data must be processed in a way that protects the privacy, dignity, and rights of individuals, in line with current data protection legislation and the school's safeguarding responsibilities.

Communication Technologies							
	Staff & Other Adults			Learners			
	Allowed	**Allowed at certain times**	**Allowed for selected staff**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with staff permission**
Mobile phones may be brought to school.	✅	✅	✅				✅
Use of mobile phones in lesson time.		✅					✅
Use of mobile phones in social time.	✅						✅
Taking photos on mobile phones/cameras.			✅				✅
Use of other mobile devices e.g. tablets, gaming devices.	✅						✅
Use of personal email addresses in school, or on school network.							✅
Use of school email for personal emails.							✅
Use of messaging apps.							✅
Use of social media.							✅
Use of blogs.							✅

When using communication technologies, the school considers the following as good practice:

- Staff and pupils should therefore use only the school email service to communicate

with others when in school, or on school systems.
- Users must immediately report to the Digital Leader in accordance with school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening, or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and in content. These communications may only take place using the official (monitored) school system Teacher to Parent text system or teacher emails (and then the Head teacher should be cc'd in). Personal email addresses, text messaging or social media must not be used for these communications. The Headteacher MUST be CC'd into any communication emails between parents and staff.
- Whole class/group email addresses may be used in FL, while pupils in KS2 will be provided with individual school email addresses for educational use.
- Pupils will be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information will not be posted on the school website and only official school email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities may be held responsible for the acts of their employees in the course of their employment. Staff members who engage in harassment, cyberbullying, discrimination (e.g. on the grounds of sex, race, disability, religion, or sexual orientation), or defamation may render the school or local authority liable. Reasonable steps must therefore be taken to prevent foreseeable harm.

The school provides the following measures to minimise risks of harm to pupils, staff, and the wider school community through social media and online presence:

- Updates on: Acceptable Use, Social Media Risks, Privacy and Security Settings, Data Protection, and Reporting Issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.
- Regular risk assessments covering safeguarding, reputational, and legal risks.

School staff should ensure that:

- No reference is made on personal social media accounts to pupils, parents/carers, or other members of the school community.
- They do not engage in online discussions about personal or sensitive matters relating to the school community.
- Professional boundaries are maintained at all times, and personal opinions are not presented as those of the school or Local Authority.
- Privacy and security settings on personal social media profiles are reviewed regularly to minimise the risk of loss or misuse of personal information.
- They do not accept or request pupils as contacts/friends on personal social media accounts, in line with safeguarding best practice.
- They use professional channels (e.g. school email, school-managed platforms such as Hwb or Teams) for all communication with pupils and parents/carers.

School's Professional Use of Social Media:

- Official school social media accounts will only be used for educational purposes, parental communication, and school promotion, and will be administered by designated staff.
- All content posted on official school platforms will comply with the school's Safeguarding, Data Protection, Communications, and Digital Images Policies.

Key Principle:
Staff must act as role models in their online conduct. Social media should be used responsibly and professionally, with safeguarding and data protection as the highest priorities.

Unsuitable & Inappropriate Activity

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:					
	Acceptable	**Acceptable at certain times**	**Acceptable for nominated users**	**Unacceptable & possibly illegal**	**Unacceptable & Illegal**
Child sexual abuse images – the making, production or distribution of indecent images of children contrary to The Protection of Children Act 1978.					✗
Grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003.					✗
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008.					✗
Criminally racist material in the UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) contrary to the Public Order Act 1986.					✗
Indecent images & videos (Pornography)				✗	
Promotion of any kind of discrimination.				✗	
Threatening behaviour, including promotion of physical violence or mental harm.				✗	
Any other information, which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.				✗	
Creating or propagating computer viruses or other harmful files.				✗	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet).				✗	

Online gaming – educational.	✅				
Online gaming – non-educational		✅			
Online gambling.				❌	
Online shopping/commerce only during break times and before/after school.		✅			
File sharing.	✅				
Use of social media – personal accounts				❌	
Use of messaging apps – personal accounts.				❌	
Use of video broadcasting e.g. Youtube.				❌	

Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see 'User Actions' above).

- All safeguarding concerns are reported immediately to the Designated Safeguarding Lead (DSL) and recorded in **My Concern**.
- Data protection incidents must be reported to the school's Data Protection Officer (DPO) within **24 hours**. Where a breach meets the threshold for notification, the DPO will ensure that the Information Commissioner's Office (ICO) is informed within **72 hours**.
- Concerns involving suspected online grooming, exploitation, or other criminal activity must be escalated promptly to the police and/or the **Child Exploitation and Online Protection Centre (CEOP)**.
- Parents/carers are informed of incidents where appropriate, in line with safeguarding and data protection responsibilities.
- The Headteacher and DSP maintain oversight of all incidents, ensuring that patterns are monitored and reported to governors where necessary.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flow Chart for Responding to Online Safety Incidents and report immediately to the police.

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see 'User Actions' above).

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible, or, very rarely through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the 'url' of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for further investigation. These may be printed, signed, and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether the concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - o Internal response or discipline procedures
    - o Involvement by Local Authority or national/local organisation (as relevant)
    - o Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:
    - o Incidents of 'grooming behaviour'.
    - o The sending of obscene materials to a child.
    - o Adult material, which potentially breaches the Obscene Publications Act.
    - o Criminally racist material.
    - o Other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

Technical Compliance

The school complies with Cardiff Council's Schools IT **Code of Connection** and associated security standards, including the use of approved filtering, firewall, and monitoring systems. Filtering logs are reviewed regularly by the Digital Lead and the Designated Safeguarding Lead (DSL), and concerns are escalated through the LA Schools IT portal. Technical queries and suspected breaches are reported promptly to the Local Authority IT support service.

Information you will find around our school:

Rhydypenau Primary School
Keeping safe when I use technology

When I use technology or go online:

- I am kind and polite.
- I take care of the equipment.
- I only use technology for the things my teacher has told me.
- I am trying to learn my password.
- I ask people before I take their photo or video.
- I wear headphones in my online lessons.

I tell my teacher if:

- I am upset about something I see.
- I think someone else is upset by something they see.
- I broke one of our rules.
- I see someone else breaking one of our rules.

Rhydypenau Primary School
PUPIL ACCEPTABLE USE POLICY KS2

This is how I stay safe when I use technology in school, and at home for my school work:

- ✓ I think carefully about what I say and do when I communicate with others and have high standards of behaviour when I work online.
- ✓ I am always kind and behave just as I do when I am working with people face to face.
- ✓ I never contact someone outside of our school by email, or using any other online communications, unless my teacher has given me permission and I have copied them into the communication.
- ✓ I am responsible. I only use technology when I have been given permission, and I only use it for my work.
- ✓ I use the sites I have been given - I never go to sites that are not about my school work or that I have not been given permission to use.
- ✓ I try to learn my password, so I can log in by myself. I keep my password a secret.
- ✓ I take care of the school technology equipment and the school network.
- ✓ I don't take photos or record other children or teachers unless they know I am doing it and they have given me their permission.
- ✓ When I am taking part in live streaming sessions involving groups of children I wear headphones.
- ✓ If I bring a device that can receive/ send communications to school I must give it to my teacher at the beginning of the day and collect it at the end. (Phones, watches etc)

I speak to a teacher if:

- ✓ If I see something that upsets me when I am working online.
- ✓ If I see someone else upset by something they see online.
- ✓ I make a mistake and post something I shouldn't or break one of our rules.
- ✓ If I see someone else making a mistake or breaking one of the rules.

Rhydypenau Primary School
Parent and Carer Acceptable Use Policy

Parents/ carers are responsible for:

- Supporting the school in promoting good online safety practice.
- Following the school policies related to online safety.
- Talking with their children about the pupil online safety agreement and encouraging them to follow it.
- Working with the school to educate and support pupils when they are involved in, or affected by, incidents regarding online safety.
- Ensuring they are aware of the permissions they have given for their child and updating them as necessary.
- Acting as good role models when using social media, publishing materials online and communicating with others online.

Taking and use of photographs

Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases, protection, these images are not to be:

- published/made publicly available online (e.g. social networking sites/ websites)
- commented on to include names of children/staff

Parents should not take photographs of staff or children outside their family without staff or parental permission.

Bringing Communications Devices to School

Many devices now send/ receive communications (e.g. emails, phone calls, texts etc) These include (but are not limited to) mobile phones, watches, music players, glasses. Children can only bring these devices to school with permission from the head teacher and with the understanding they cannot be used in school. They will be handed to the class teacher at the beginning of the day, and collected at the end. If devices such as watches need to be used in school they must be set in such a way that communications cannot be made from or to them.

Social Media

Our aim is to work together with parents and carers to provide the best educational experience for the children in our care. Parents/carers:

- Should make complaints through official channels not on social networking sites.
- Should not post malicious or fictitious comments on social networking sites about any member of the school or any member of the school community.
- Parents should not post pictures on social media of staff members or children other than their own, without prior permission.
- Act as role models for their children in their own use of social media.

Acceptable Use Community Users

We want to protect you, our pupils and our staff while you are working at Rhydypenau Primary School and keep all our community safe.

Please read and sign this acceptable use document to ensure you stay safe while working at our school.

- I use any online systems responsibly and legally, ensuring that what I present, share or produce will be of educational value and acceptable to the school community.
- While I am at school I use devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users.
- I will ensure that I have viewed any material I intend to use with pupils prior to using it in the school.
- I may use my own laptop or chrome book and sign on to the public network or a teacher will allow me to use the class computer for my work. If I use my own laptop I ensure it is appropriate for school use.
- I do not use any external drives on the school network.
- I understand that my use of school systems, devices and digital communications will be monitored.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will ensure that if I take and/or publish images of others I will only do so with their permission.
- I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will ensure that I have permission to use the original work of others in my own work.

I understand that if I fail to comply with this Acceptable Use Agreement, the school/college has the right to remove my access to school systems.