Pontnewydd Nursery and Primary School

Acceptable Use Policy

(Social Media Policy)

DOCUMENT CONTROL

Title:	**Acceptable Use Policy**		
Document Owner:	**Head teacher**		
Document Author:			
Reference:	PPS	**Retention Period:**	**Until next review**
Document Classification:	Official	**Location:**	School
Version / Status:	1 Live	**Approved by:**	SCHOOL GOVERNORS
Current Issue Date:	April 2025	**Next Review Date:**	April 2028

REVISION HISTORY

Issue Date	Version / Status	Reason for Change	Changed By:
June 2019	1.0	Policy Implemented	Information Governance
May 2021	2.0	Change to UK GDPR/Information regarding Zoom (Section 10) Insert Hwb links to online learning(Section 11)	AP
Nov 2023	2.0	Three year review.	AP

Table of Contents

DOCUMENT CONTROL 2
REVISION HISTORY 2
1. PURPOSE 4
2. SCOPE 4
3. PRINCIPLES 4
4. OBJECTIVES 5
5. RESPONSIBILITIES 5
6. LEGISLATION & KEY REFERENCE DOCUMENTS APPLICABLE TO THIS POLICY 5
7. MONITORING AND REVIEW 6
8. COMPLIANCE 6
APPENDIX 1 – ACCEPTABLE USE PROCEDURES (AUP) 7

1. PURPOSE

The purpose of this Acceptable Use Policy (AUP) is to:

- Outline the acceptable use of computer/ICT equipment at Pontnewydd Nursery and Primary School "The School" and including Bring Your Own Device (BYOD) devices.
- The policy set outs the parameters, boundaries and conditions of workplace and personal use to protect the interest of both the School and users.
- This policy sets out the viewpoint and intent of the School on acceptable use of information systems/services and to minimise the risks associated with accidental or malicious abuse of the equipment, information, and associated services.
- The overriding principle is that the use of the School's equipment and systems are for School business use whereby personal usage must not interfere with an individual's work activity and responsibilities.
- These requirements/rules are in place to advise and protect both the employee/user and the School. Inappropriate use exposes the School to risks including virus attacks, compromise of network systems and services, and legal issues to which non-compliance could mean disciplinary investigation against the user.
- In circumstances where a School employee/user or worker is utilising the equipment or systems of another organisation within the course of their employment, this policy is supplemented by the provisions and restrictions set out by that organisation. Those employees are expected to obtain copies of any relevant IT/ equipment usage policies either directly or through their line manager and apply these when using systems and equipment owned/loaned by the organisation

2. SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct School business or interact with internal networks and systems, whether owned or leased by the School, the employee, or a third party.

The policy applies to:

- Employees, whether office based or working via remote access, including governors, contractors, volunteers, agencies and partner organisation operating on behalf of the School.
- All equipment that is owned or leased by the School.
- All resources owned by the Council including that which is held/accessible on BYOD devices, and managed by the Intune Company Portal (MDM

3. PRINCIPLES

To establish and maintain the guidance of acceptable working practices to protect the School and those users carrying out work on its behalf.

- Ensuring that all members of staff/governors and third party users are aware and understand their personal responsibilities of acceptable/non acceptable use of information and systems controlled by the School.
- Ensure there is a concise Acceptable/Non acceptable guidance document to support this policy which is available to all users and follows as **Appendix 1** to this policy.

4. OBJECTIVES

The objectives of this policy are:

- To ensure the confidentiality, integrity and availability of information is adequately protected.
- Enable staff/governors and all third party users to utilise the information, equipment and networks appropriately and thereby ensure the School is not compromised through inappropriate use as set out within Appendix 1 of this policy.
- Support, advise and protect staff/governors and all third party users from non-compliance and potential disciplinary action.

5. RESPONSIBILITIES

<u>Governors/Head teacher</u>

- The schools equipment, networks, information and systems are the responsibility of the Governors/ Head teacher.
- Day to day ownership sits with the Head teacher.

All Staff/Governors 3rd Parties

- Maintaining the security, confidentiality, integrity and availability of all School information, equipment, and systems is the responsibility of all users employed or contracted to undertake work on behalf of the School identified in 2 above.
- Are responsible for adhering to the Acceptable Use Policy and related procedures/guidance as well as undertaking any relevant training/awareness provided.
- Specific Information Governance responsibilities are detailed in the Information Governance Management Framework overseen by the Head teacher.

6. LEGISLATION & KEY REFERENCE DOCUMENTS APPLICABLE TO THIS POLICY

(Please note this list is not exhaustive)

The School will abide by all relevant UK and EU legislation and the following key documents (where applicable)

- UK General Data Protection Regulation
- The Data Protection Act (2018)
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000 (RIPA)

Policies

- Data Protection Policy
- Information Data Loss Policy
- Information Security Policy
- Retention Policy
- Secure Destruction Policy
- Password Policy and Procedures

7. MONITORING AND REVIEW

The Head teacher/Governing Body will monitor/implement and review this policy.

This policy will be subject to review when any of the following conditions are met:

- Content errors or omissions are highlighted.
- Where another standard / guidance issued conflicts with the information in this policy.
- There will be an initial 1 year review from policy implementation
- Thereafter reviews will be scheduled on a 3 year basis from the date of approval of the current version.

8. COMPLIANCE

Failure to comply with the Acceptable Use Policy could result in disciplinary action and in serious cases resulting in termination of employment

- The Information Security Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

- Any exception to the policy must be approved by the Head teacher/Governing Body.

APPENDIX 1 – ACCEPTABLE USE PROCEDURES (AUP)

Pontnewydd Nursery and Primary School is a modern School that utilises a wide range of networks and equipment dependent upon the functions required. The appropriate use of the Schools information/data assets is critical to maintain daily operating business.

Please note that the School reserves the right to monitor and access user's accounts for business purposes at any time.

Each time you access the School's network you will be asked to accept that you have read the Information Security Procedures Statement & Acceptable Use Policy and that you agree to comply with them.

In addition, the Head teacher may add to these requirements at any time to further secure the Schools networks and procedures.

You must at all times comply with the Schools policies/procedures/guidance and deliberate or malicious use by you of the Schools assets **may lead** to a disciplinary investigation and further action being taken in accordance with the School's Disciplinary Policy and Procedure.

This Appendix should be read alongside the Acceptable Use Policy (AUP) and its intent is to guide and protect you and inform you to what you can and cannot do. It's not a catch all and if you are unsure of any aspect you should seek the guidance of the Head teacher and the Data Protection & Information Governance Officer on 01495 766257 dpa@torfaen.gov.uk

.

The appendix is set out in sections and indexed below for ease of reference and hyperlinked.

Index

1. Accessing the School's Network
2. Passwords
3. Use of email
4. Use of secure email accounts
5. General use of the Internet explained
6. School internet must do's and don'ts
7. Security
8. Data processing and reporting breaches
9. Social Media & Blogging
10. Streaming & Video Messaging
11. Distance Learning
12. Professional Communciation
13. Handling personal information
14. General – Bring Your Own Device

15. Handling Abuse

16. Acceptuable Use Policies

1. **Accessing the Schools network drives**

This is where the School holds the electronic information to undertake day to day business. You will as an employee have access to network drives which consist of a shared drive and a personal space. In addition, schools will also have access to Hwb which is a digital platform for learning and teaching and holds a collection of online tools provided to all schools in Wales by the Welsh Government.

When accessing these drives, you **must** –

- Have permission, your Head teacher/Bursar would have completed a User Access Request (UAR) to allow you to access certain areas of the system to undertake your job.
- Accept and agree the Information Security/ Acceptable Use Statement on the login/splash screen when you first log in and always log in with your own credentials.
- Lock your computer or mobile device when unattended by using the Windows Key  & L or Ctrl, Alt & Delete, & Enter. At the end of the working day you must lock or shut your system down.
- Save (transfer) school documents/information to the shared drive do not keep in your personal area. Only use the C drive on an encrypted machine, and with approval from your head or bursar as a temporary measure until you can transfer the file to the relevant corporate drive as it is not backed up and is not secure.
- Report suspected Malware/ransomware/activity of any kind on your computer equipment to the SRS Helpdesk on 01495 766366. Following, you must power down immediately and unplug your hardwired Ethernet cable.
- You must not change the configuration of the device or knowingly remove or install any software to the device that has not been approved.

When accessing these drives, you **must not** –

- Share your log in details or allow anyone to use your user name and password. The School can arrange for an appropriate shared inbox - please contact the SRS Helpdesk on 014795 766366 to set up with a UAR completed with your Head teachers approval
- Access areas in relation to previous roles unless required to do so for business purposes.
- Breach security by disrupting any network/s, accessing information/systems/networks for which you do not have authorisation or no legal basis to access, access prohibited server/accounts.
- Connect any unauthorised device to the schools network drives.
- Save non business/ personal photos, videos, music, audio, media files on to any of the school's network drives.
- Deliberately or with intention knowingly introduce any form of virus or Malware onto the School's servers/networks.
- Do not use personal devices or personal accounts for the school's business or to try and access any corporate network drive. However staff should talk to the Education Team about the correct way of setting up services using a school-specific account.

2. Passwords

You will be required when utilising the Schools systems to enter a complex password. This not only protects the School and you but is a requirement for the School to access and comply with the Public Service Network (PSN) security network provided through the Central Government Cabinet Office for all public services. Without PSN accreditation, the School cannot undertake its business.

You must -:

- Have a User ID (usually your payroll number) and complex password to connect to the Schools networks and systems.
- Change your password every 90 days, you must be connected to an Ethernet cable when changing.
- Use a strong password that has a minimum 8 characters, combines Uppercase, lowercase, numeric & special characters and should not be obvious, an example of a strong password is M4nChe5ter11td#

You must not -:

- Request your Passwords to never expire
- Share your username/password or ignore password change requests
- Keep generic passwords or use weak passwords e.g. Password1
- Use the same password across multiple systems
- Do not write your passwords down or store passwords insecurely

3. **Use of email**

Email is critical to the business of the School and it drives our everyday activity. Without it, all school business would grind to a halt. Every email that enters and leaves our systems, can be monitored and the information they hold belongs entirely to the School as it goes through our network. People who have been granted access to our systems will be given a School email address for business purposes.

When using email **you must -:**

- Use your email that ends @ Torfaen.gov.uk /school specific email address and/or schoolsedu.org.uk when sending emails for the Schools business purposes.
- Ensure the email address to which you are sending information is correct, to check, hover over the address to display it in full.
- Ensure that any email you send on behalf of the School is professional, appropriate and in line with the Dignity at Work Policy
- Use caution when receiving emails from unknown or unusual email addresses. If you receive a suspect email you must query this with the IT Helpdesk on 01495 766366 or contact security@srswales.com / security@torfaen.gov.uk / dpa@torfaen.gov.uk
- Use caution with email links as these may contain malware/viruses, hover the mouse over the link to verify the address stated and is you are concerned follow the process above.
- Ensure your email signature is bilingual in Welsh/English and contains contact details in line with the corporate standard.
- Report email data breaches immediately to the Head teacher who can then report to the Data Protection & Information Governance Officer (DPA@torfaen.gov.uk)
- Use the VPN facility when working remotely to securely log in, using your school assigned device

Remote access to emails is covered under section 5 – Use of the Internet

When using email **you must not -:**

- Send any business emails or attachments from your School accounts to your own personal accounts e.g. your personal Hotmail/gmail/AOL or other private email domain/accounts particularly those that are private, confidential and/or sensitive in nature.

  Why is this of particular importance? – When emails leave the Schools Public Services Network (PSN) to a personal account they are no longer protected and can be hacked or intercepted as your home/private email may not be protected to the same degree as through the SRS networks. This leaves you and the School open to a potential attack and/or investigation from the Information Commissioners Office (ICO).

- Use your School email address for personal use unless authorised by your Head or bursar.
- Send unprofessional, unsolicited or chain emails
- Click on any suspect links if you do so report it immediately to the ICT helpdesk on 01495 766366 or security@srswales.com / security@torfaen.gov.uk / dpa@torfaen.gov.uk
- Promote your own or anyone else's personal business, political or religious interests
- Do not forge or misuse any email header information
- Use your corporate signature for non-business emails

4. Use of Secure Email Accounts

Torfaen County Borough Council and School email system is Transport Layer Security (TLS) accredited.
Information sent by the School via email can be intercepted once it leaves our network and therefore when we send personal information to an individual or organisation we must make every effort to ensure its security.
Torfaen uses the Micorsoft Onedrive facility to send and receive information securely to those who are not TLS accredited.
If you are sending to a new contact/organisation:

- Contact security@srswales.com to verify the email address is accredited as being secure
- If they are not accredited you will need to password protect attachments ensuring no personal information is included within the body of the email or send via OneDrive

- Generally email addresses ending .gov.uk/pnn.uk/wales.nhs.uk are secure however you must be cautious as these can be 'spoofed' and you should hover over the address to reveal the true sender

  If you are sending to an individual with a private email address such as yahoo/AOL/Sky/etc follow instructions as above

- If you have to transfer information other than by email and use a USB memory stick, please ensure that this has been purchased via SRS and is encrypted. You should password protect the stick and send /relate the password previous to sending the information.

5. General use of the Internet

The internet is a business-critical tool used by the School to deliver its daily business. It should not be for personal use.

The School reserves the right to monitor Internet usage to include the monitoring of broadband use, access any data that you search, write, send, receive or store. Monitor usage while connected to the network or while using VPN. Accessing/Monitoring information will normally occur in consultation with the Head teacher and/or HR if there is reasonable cause.

NOTE: **The School does allow staff/users to access the network for personal use during official breaks and when signed out, such as lunch breaks or at other times subject to approval from your Head teacher subject to certain conditions identified below:**

6. School Internet

When using the Internet **you must** -:

- Ensure all business documents/information/communication is sent through the schools approved network.
- If the information is of a sensitive nature this should be password protected and a separate email sent to the recipient requesting a telephone call to receive the password/or include the password to open the attachment in a separate email to avoid business delays.
- Ensure communication and information exchanges should directly relate to missions, goals and work tasks of the School
- Only use for research, advisory, standards analysis and professional society or development activities

- Order goods or services within the guidelines of the authority's standing orders.
- Use Office 365 work accounts, Hwb accounts and other approved SRS accounts where available

When using the internet **you must not** -:

- Deliberately download software/malware/viruses or other ware that will disrupt and affect the School's business
- Save personal photos, videos, music, audio media files
- Access, write, send, read, receive content considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any person or organisation
- Undertake the following functions/activities (downloading or accessing) including but not exclusive to -:

List of Unacceptable Actions-:

- Activity which may put the School at risk
- Offensive, obscene, indecent , racist or sexist information
- Conducting non approved business
- Illegal activities
- Use of material protected by trade secret
- Unauthorised political activity
- Use of information protected by copyright without consent
- Usage of School logos or trademarks for non-business purposes.
- Activities that knowingly cause congestion/disruption to networks and systems
- Malicious attacks that attempt to harm/destroy systems/data
- Break through security controls
- Personal use of YouTube, Netflix, TV catch-up channels, other radio/tv subscriptions
- Download games/audio midi files
- Intercepting data
- Port or security scanning
- Access chat rooms (unless work purpose)
- Offering of products
- Unauthorised use, installation, copying or distribution of copyrighted, trademarked, or patented material
- Downloading software without an appropriate licence
- Making copies of computer software owned or licensed by the School

- Installing software onto Torfaen systems without prior written approval from the Information Security Team/SRS
- Releasing personal data without authorisation. Personal data should not be published on the internet unless appropriate authorisation has been granted from the Head teacher.
- Copying copyrighted data
- Distributing any 'pirated material'

7. Security

Security of our systems is paramount and significant resource is spent annually to ensure malware and ransomware and other cyber-attacks are identified and managed as quickly as possible and we resume business as usual as quickly as possible. To enable this to function, security is continually monitored. Users of our systems are pivotal in supporting the security aspects of our work.

You **must** -:

- Report any known/potential security issues to the Security Team at Shared Resource Services (SRS) on 01495 766366 security@srswales.com / security@torfaen.gov.uk / dpa@torfaen.gov.uk
-
- Report loss/theft of a corporate device or approved BYOD immediately to the SRS Service Desk on 01495 766366

You **must not** -:

- Ignore security flaws, faults or weaknesses in systems
- Transfer data/information outside of the School unless you have been given specific authority to do so using the appropriate channels
- Perform changes to IT systems/information without prior authorisation
- Access information, systems, services, applications, servers etc. for any reason other than to complete tasks assigned to you during your job role
- Allow persons not employed by the School to view information or use devices provided by the School or its partners without authorisation
- Download School data/transfer of information on termination of employment. This data and Information belongs to the School

8. Data processing and reporting breaches

The School is required under the UK General Data Protection Regulation to notify the Information Commissioners Office (ICO) annually what information is being processed. Each school must register and pay a fee to the ICO and will be given a registration number. Failure to update the register is a criminal offence. You must ensure that contractors (working for your service area) meet the standards of the General Data Protection Regulations when processing personal information on behalf of the School

- Do not report information/data/security breaches **directly** to the ICO. The Head teacher should be informed and work with the Data Protection & Information Governance Team who will work through the breach and decide if the ICO need to be informed. Contact Data Protection Team at DPA@torfaen.gov.uk

- You must try and retrieve the information as soon as you are aware of the breach

- You must use the templates available to manage Information/Data Loss breaches

- You should undertake the mandatory Cardinus e-learning Data Protection Awareness Course by following the link sent to your Torfaen.gov.uk email address and/or follow the data protection SWAY training sent from your Head or bursar.

9. Social Media & Blogging

This relates to online tools, websites and services that share content, profiles, opinions, experiences, interests and media, some schools use this to publish policies and school information e.g. Twitter, Snapchat, Facebook, school website

You **must -:**

- Ensure anything you post is allowed to be in the public domain, distribution of material cannot be controlled once posted
- Be aware of geo-locations applications as these reveal your real time location
- Use privacy setting to reduce personal information being accessed by unintended recipients

- Blogging is acceptable provided that it is done in a professional manner that will not bring the School into disrepute and is subject to monitoring
- Ensure posts from school staff to newsgroups should contain a disclaimer stating that the views contained are their own and not those of the School unless for normal business duties

You must **not -:**

- Express strong personal views on accounts that identify you as an employee of the School
- Attribute any personal views to the School when blogging or using any other forms of social media
- Defame or disparage the School its customers, clients, business partners, suppliers, vendors, or other stakeholders
- Breach the School's Dignity at Work Policy
- Breach the Data Protection Act (DPA) or the UK General Data Protection Guidelines
- Breach other laws or ethical standards
- Use corporate logos, brand names, slogans or other trademarks, confidential or proprietary information without School permission

Personal Use of Social Media outside of School

Staff

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school permits reasonable and appropriate access to private social media sites.*

Pupils

- Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account. (Exceptions are made for pupils/staff who have recognised relationships or work at the school).
- The school's education programme should enable the pupils to be safe and responsible users of social media.
- Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

10. Streaming, video and instant messaging

- Video and music streaming can be subject to copyright and licence agreements, these must only be used for business purposes/training such as researching video/training on YouTube
- Microsoft Office Teams and SKYPE is to enable virtual meetings. The same principle applies to instant messaging and should not be used for personal use
- You must not access the following for personal use when connected to the corporate network, You Tube, Netflix, TV catch-up channels, other radio/tv subscriptions, download games/audio midi files

Microsoft Office 365/TEAMS

<u>Video Conferencing/Virtual Meetings</u>

- Microsoft Teams is a software application that enables virtual meetings. Training and guidance documents are available through the ICT Training and Support section on SWOOP.

Recording of meetings/calls (audio and visual)

You must **only** record meetings/calls where a business need has been identified and approval has been obtained from the Head teacher.

- Once the specific request has been approved you **must:**
- Inform participants that the meeting is being recorded and that information is not to be shared in any format with individuals not connected with the meeting
- Move the recording from the Chat area once finished, by selecting the download button, it will save to your Downloads folder
- Then immediately transfer the recording to the relevant network drive .
- You can then transpose the audio meeting to a written report, once this is done delete the recording
- If you are keeping it in audio format be aware that all recordings are school business records and therefore form part of Business Continuity, Information Management/Governance and are auditable records, they could also form part of a Subject Access Request (SAR) or a Freedom of Information Request (FOI).
- Follow the departmental retention guideline for the specific type of record
- Ensure the record is searchable and available as all recordings are subject to SARs and FOIs. Where redaction is required there must be a suitable method in place to achieve this at service area level.
- School/Council approved facilities for Video conferencing should **only** be undertaken through Microsoft Teams or SKYPE. Zoom may only be used under certain circumstances (please see paragraph below). Due to security controls, other video conferencing applications have been deemed unsecure for the Schools use.
- Guidance pertinent to homeworking and the COVID19 situation are available in the Information Management section on SWOOP.
- You must not access a meeting via another person's calendar appointments unless invited or authorised to do so.
- Always exercise caution when receiving an invitation in the same way as if you had received an unsolicited email/link
- Follow the guidance around the Bcc facility when inviting external participants to ensure the security of the meeting

Instant Messaging

- Microsoft Chat is an instant messaging facility with a limited retention period

- It must not be used for business purposes or contain personal data therefore you must use an alternative method (such as email)
- All conversations are auditable and subject to FOIs and SARs

Channels

- When using the Teams function you have the option to create Channels and post collaborative documents.
- All posts within a Teams Channel remain for the life of that Team and would need to be included in any SARs/FOIs received.
- The Teams Channel is only a temporary repository and any information needs to be transferred to the school network drive.

All Teams Channel posts are school business records and therefore form part
of Business Continuity, Information Management/Governance and are auditable records

Zoom

The Zoom platform carries significant risk to the corporate and school network as is it unsecured and as such has strict controls in place which you must adhere to:

You **must:**

- Obtain prior approval from the Head teacher and SRS
- Participate in Zoom meetings or training by INVITATION only
- Access only through your work secured browser
- Disclose your name, title and organisation only and not share other personal information
- Ensure your privacy by using headphones and apply backgrounds where necessary

You **must not:**

- Host a Zoom meeting or training the preferred platform is Microsoft Teams
- Download the Zoom App from a virtual store
- Share any school documentation, service user details or personal information
- Disclose any personal/sensitive information in the Chat facility
- Access a Zoom meeting or training through someone else's calendar
- Remain in the meeting if an uninvited participant is detected – you must leave and wait for the organiser to make contact

The councils security systems will not allow staff to join Zoom meetings by clicking on the meeting URL.
Search for Zoom.us on your browser and click "Join a Meeting" using the meeting ID and passcode you have been sent. You will get a warning message the first time you try to access the site – please read carefully and click Ok to proceed.
You will be asked if you want to join the meeting by downloading the client, or through your browser. DO NOT download Zoom onto your computer. This version of the platform does not have any security feature. If you have already installed the Zoom client please refer to the attachment and manually uninstall it.

11. Distance Learning

Due to the Covid pandemic schools under direction from Welsh Government implemented live streaming and video conferencing to deliver lessons to pupils. Please see the attached link developed via HWB which give guidance for schools on the safe delivery of lessons.

Live-streaming and video-conferencing: safeguarding principles and practice - Keeping safe online - Hwb (gov.wales)

Live lessons - Hwb (gov.wales)

12. Professional Communciation

Professional communications are those made through official school channels (hwb emails/TEAMS, Hwb Shared Drives, Whatsapp PPS, telephone) posted on a school account or using the school name.
All professional communications are within the scope of this policy.

13. Handling Personal Information

As a public body we collect and process personal information on a daily basis, this can be held in electronic, paper or digital format. The main legislation applicable is the Data Protection Act 2018 and the UK General Data Protection Regulations and staff should refer to the Council's Information Management policies and procedures held on SWOOP.

14. General – Bring Your Own Device

- All school owned devices must be returned upon termination of your employment

- Any Council apps such as Intune Company Portal (MDM) which has been downloaded onto your personal device and used for accessing the corporate or school network must be deleted upon termination of your employment. For further information relating to BYOD refer to the Council's Information Management policies and procedures held on SWOOP.
- No files should be saved to personal devices except in the secure area allocated. These files will be deleted when the app is removed so must be transferred to your school area on termination
- You must delete the Intune Company Portal (MDM) app used for accessing the network/information on your personal device if you take your BYOD outside the EEA, and reinstall it on your return. As stated above this will also delete all files saved in the secure corporate area
- The School/Council reserves the right to withdraw the 'personal usage' facility of School/Council IT equipment without notice to include personal mobile phones and devices
- Work spaces must be cleared/locked away of all sensitive, personal, confidential documents in line with Alternative Workplace Strategy
- You must only purchase software through the Shared Resource Service and have it installed by SRS employees
- You must not disclose third party information without appropriate legislation/purpose/consent

- **Recruitment** - Persons conducting interviews must arrange to virus check memory sticks and ensure candidates cannot access corporate information/systems

- **Retention** - You must ensure that you hold the data for the prescribed timeframe as in line with the Retention Guidelines, information for permanent archive should be passed to Gwent Archives.

- **Disposal** - You must dispose of information in the appropriate method considering

- Retention Guidelines
- Secure Disposal Policy
- Permanent archive
- Insurance purposes

- Paper copies have to be securely shredded.

- IT equipment needs to be disposed of via the Shared Resource Services and CD's/USB's containing personal information must be securely destroyed.
- Please refer to the BYOD Policy and Guidance if you recycle/sell your personal device and you have used it to access school files

- **International Transfer** - You must implement additional measures when transferring personal data outside of the European Economic Area to comply with the UK General Data Protection Regulations. You must liaise with the Data Protection & Information Governance Officer.

15. Handling Abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.
- Stakeholders will be offered support in handling abuse and offered advice which may involve the school/governors or police if necessary.

16. Acceptable Use Policies - Older pupils/Younger Pupils/Staff and Governors/Parents and Carers/Communtiy Users

Pupil Acceptable Use Agreement Template – for older pupils

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the *school* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission.
- I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. Mobile phones are not to be used on site and must be stored turned off in a teacher's office/cupboard or at the main office. Failure to do so results in banning of bringing devices to school for a week. term and then indefinitely formed on a 3 strike basis. (Shared with pupils/parents/staff at the beginning of the year and reminded throughout).
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the *school/academy* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, banning of bringing in devices, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the *pupil* acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the *school* systems and devices (both in and out of school)
- I use my own devices in the *school* (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Pupil Acceptable Use Policy Agreement – for younger pupils – Foundation Phase

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong

- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child): _____

(A copy to be shared with parents only – no signature required.)

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school/academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students/pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school/academy* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school* systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.see Social Media Policy
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. *(guidance shared in annual training and available on School Drive for reference).*
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school/academy*:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems, unless permissions have been sought by SLT/or they have been used to create accounts for educational purposes.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school/academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies or [permission sought by SLT/SRS.
- I will not disable or cause any damage to school/academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Academy/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school/academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school/academy*:

- I understand that this acceptable use policy applies not only to my work and use of school/academy digital technology equipment in school, but also applies to my use of school/academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school/academy
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors referral to the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: _____

Signed: _____

Date: _____

This form (electronic or printed) Autumn Term 2024
Who will have access to this form. Office Staff/SLT/Safeguarding Leads/Online Safety Lead/Link Governor
Where this form will be stored. Google Forms – HWB
How long this form will be stored for. 1 year
How this form will be destroyed. Deleted from Hwb systems.

Acceptable Use Agreement for Community Users Template

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and 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. This agreement will also apply to any personal devices that I bring into the school/academy:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- 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 not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school/academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school/academy has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

This form (electronic or printed) Autumn Term 2024
Who will have access to this form. Office Staff/SLT/Safeguarding Leads/Online Safety Lead/Link Governor
Where this form will be stored. Google Forms - HWB
How long this form will be stored for. 1 year
How this form will be destroyed. Deleted from Hwb systems.

Acceptable Use Agreement for Community Users Template

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices

- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and 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. This agreement will also apply to any personal devices that I bring into the school/academy:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- 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 not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school/academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school/academy has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

This form (electronic or printed) Autumn Term 2024
Who will have access to this form. Office Staff/SLT/Safeguarding Leads/Online Safety Lead/Link Governor
Where this form will be stored. Google Forms – HWB
How long this form will be stored for. 1 year
How this form will be destroyed. Deleted from Hwb systems.