Crownbridge School

Acceptable Use Policy

Version 1.0 Live

DOCUMENT CONTROL

Title:	**Acceptable Use Policy**		
Document Owner:	**Head teacher**		
Document Author:			
Reference:	SCHOOL – IG007	**Retention Period:**	**Until next review**
Document Classification:	Official	**Location:**	School
Version / Status:	1 Live	**Approved by:**	SCHOOL GOVERNORS
Current Issue Date:	July 2019	**Next Review Date:**	July 2020

REVISION HISTORY

Issue Date	Version / Status	Reason for Change	Changed By:
June 2019	1.0	Policy Implemented	Information Governance

Table of Contents

1. PURPOSE

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

- Outline the acceptable use of computer/ICT equipment at Crownbridge School "The School".
- 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 action 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 used 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**.**

All employees, governors, contractors, consultants, temporary, and other types of workers at the School are responsible for exercising good judgment regarding appropriate use of school resources in accordance with the School's policies, standards and procedures, and local laws and regulation. The requirement is of this policy to be read together with the Information Security Policy.

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.

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.
- Ensure processes are in place to manage adherence 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

Governors/Head teacher

- The schools equipment, networks, information and systems is 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.
- 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)

- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
- The Data Protection Act (2018)
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000 (RIPA)

Policies

- Data Protection Policy
- Information Data Loss Policy

Procedures

7. MONITORING AND REVIEW

The Head teacher/Governing Body will monitor the review of this policy.

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

- Content errors or admissions 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 POLICY (AUP)

Crownbridge 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 (UAP) 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 to any aspect you should seek the guidance of the Head teacher and the Data Protection & Information Governance Officer on 01495 766257.

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

Index

1. Accessing the Schools Corporate IT 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, Google etc.

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.
- Only use the Torfaen device allocated to you to access the network drives.
- 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.
- 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.

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 appropriate shared inbox - please contact the SRS Helpdesk to set up 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.
- Must not 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 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 for Head teachers, office staff and schoolsedu.org.uk for teaching staff 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.
- 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
- Use caution with email links as these may contain malware/viruses, hover the mouse over the link to verify the address stated.
- 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 PSN networks 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 line manager.
- 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
- 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. 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:**

5. Internet

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

- Ensure all business documents/information/communication is sent through the school 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
- 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 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’

6. 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

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

7. Data processing and reporting breaches

The School is required under the 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
- Paper Documentation - You must ensure that a process for securing hard copy personal data within your working area exists and is used when required; minimise the amount of hard copy information removed

from the office and secure hard copy information at all times. Following, you must securely destroy hard copy information that contains any personal/sensitive personal data (refer to the Secure Destruction Policy)

8. Social media & blogging

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

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 TCBC 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 General Data Protection Guidelines (EU) 2016/679)
- Breach other laws or ethical standards
- Use corporate logos, brand names, slogans or other trademarks, confidential or proprietary information without School permission

9. 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

- 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, YouTube, Netflix, TV catch-up channels, other radio/tv subscriptions, download games/audio midi files

10. Handling Personal Information

As a public body we frequently handle and administer personal information and there are regulations surrounding this activity.
Personal information can be held in electronic, paper or digital format. The process is extensive and covered within the Data Protection Policy.

11. General

- All School owned devices must be returned upon termination of your employment unless there are agreements in place for you to buy your device.
- The School reserves the right to withdraw the facility for any personal usage of School IT equipment without notice.
- Work spaces must be cleared/locked away of all sensitive, personal, confidential documents at the end of the working day.
- You must 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.
- You must not recycle personal information

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

Breach Templates

Attach here.