

IT Acceptable Use Policy Template

For Jamaican organizations. Prepared by Syxel Technologies Limited.

How to use this template

This template gives you a complete starting point for an IT acceptable use policy. Delete this page before you adopt it.

- Replace everything in [square brackets] with your own details, and delete sections and examples that do not apply. A business that does not allow personal devices for work, for example, can replace section 12 with one sentence saying so.
- Decide who owns the policy, who handles IT requests and who advises on personal data (your Data Protection Officer, if you have one).
- List your approved tools in the places marked: email, messaging, cloud storage and any device management software.
- This policy refers to a password policy and an AI usage policy. If you have not adopted them yet, free templates for both are available at www.syxeltech.com/resources/password-policy-template and www.syxeltech.com/resources/ai-usage-policy-template.
- Complete the monitoring table in section 18 so it describes what you actually monitor. Do not list monitoring you do not do, and do not do monitoring you have not listed.
- Have the policy reviewed by a legal adviser, in particular the monitoring and disciplinary sections, and check it fits your employment contracts and staff handbook.
- Brief staff on the policy, use the forms in Appendices A and B, and collect signed acknowledgements (Appendix C).

This template is general guidance, not legal or employment-law advice. It was prepared by Syxel Security, the cybersecurity team at Syxel Technologies Limited, with the Jamaica Data Protection Act, 2020 in mind. For help adapting it or training your staff, contact sales@syxeltech.com.

[Organization] IT Acceptable Use Policy

Policy owner	[Role, e.g. Operations Manager or IT Manager]
Approved by	[Name, role]
Version	[1.0]
Effective date	[Date]
Next review	[Date, 12 months after the effective date]

1. Purpose

This policy explains how people working for [Organization] may use our IT equipment, systems, accounts and information, and their own devices when used for work. It protects our customers, staff and organization from security incidents, data loss and misuse, and helps us meet our legal obligations, including under the Data Protection Act, 2020 (the "Act").

2. Scope

This policy applies to:

- all employees, contractors, consultants, interns, volunteers and anyone else given access to [Organization] systems;
- all [Organization] devices, including computers, laptops, tablets, phones, printers and storage devices, wherever they are used;
- personal devices used for [Organization] work, including phones used for work email or WhatsApp;
- all [Organization] accounts and systems, including email, file storage, business applications, Wi-Fi, social media pages and messaging groups used for work;
- all [Organization] information, in any format, including paper.

3. Definitions

Term	Meaning
Company device	Any computer, phone, tablet or other equipment owned, leased or provided by [Organization].
Personal device	A device you own that you use for [Organization] work, such as your own phone or laptop. Using one for work is often called "bring your own device" or BYOD.

Term	Meaning
Approved	Listed or authorized by [role] for [Organization] use, with the settings and conditions [role] sets.
Personal data	Information about a living person who can be identified from it, directly or indirectly, such as a name, address, phone number, TRN, account number, photo or voice recording.
Sensitive personal data	Personal data the Act protects more strictly, such as information about health, genetic or biometric data, racial or ethnic origin, political opinions, religious beliefs, trade union membership, sex life, and criminal offences or proceedings. See the Act for the full definition.
Confidential information	Information that is not public and could harm [Organization], our clients or partners if disclosed, such as contracts, pricing, financial records, plans and client files.
Security incident	Anything that has harmed, or could harm, our systems or information, such as a lost device, a malware infection, a phishing email someone acted on, or information sent to the wrong person.

4. Roles and responsibilities

Role	Responsibilities
Policy owner: [role]	Keeps this policy up to date, approves exceptions, arranges training and reviews the policy.
IT staff or IT provider: [name or company]	Issues and supports devices, manages accounts and approved software, applies security settings and handles incident reports.
Data Protection Officer: [name or role]	Advises on personal data, decides whether an incident is a personal data breach, and handles reporting to the Information Commissioner.
Managers	Make sure their teams know and follow this policy, approve access and equipment, and tell [role] about starters, role changes and leavers in good time.
Everyone covered by this policy	Follows this policy, protects the devices and information in their care, and reports problems straight away.

5. General rules

- [Organization] systems and devices are provided for work. Limited personal use is allowed if it is occasional, does not interfere with your work or anyone else's, costs us nothing significant and

does not break this policy.

- You are responsible for everything done with your accounts. Do not let anyone else use them, and do not use anyone else's.
- Only access the systems and information you need for your job, even if your account technically allows more.
- Do not try to get around security controls, such as antivirus, firewalls, web filters, screen locks or device management software.
- Do not use [Organization] systems for anything illegal, for harassment or discrimination, to view or share offensive or sexually explicit material, for gambling, for running a personal business, or to infringe copyright.
- If you are unsure whether something is allowed, ask [role] first.

6. Company devices

- Company devices are issued using the form in Appendix B and remain the property of [Organization].
- Keep devices in good condition and protect them from damage, theft, heat and water. Report damage or faults to [role] promptly.
- Do not let family members, friends or other people use a company device.
- Do not change security settings, remove management software, or take devices apart or to an outside repair shop. All repairs go through [role].
- Allow updates to install promptly and restart when asked. Do not postpone security updates for more than [3] days.
- Save work files to [approved storage, e.g. OneDrive or the shared drive], not only to the device itself, so they are backed up.
- Return devices when asked, and before your last day (section 20).

7. Passwords and sign-in

Follow the [Organization] Password and Authentication Policy. In summary:

- Use a long passphrase and a different password for every work account, stored in [the approved password manager].
- Use multi-factor authentication wherever [Organization] has turned it on, and never approve a sign-in prompt you did not start.
- Never share your password or MFA codes with anyone, including colleagues, managers or IT.
- Lock your screen whenever you step away (Windows key and L, or Control, Command and Q on a Mac).

8. Email

- Use your [Organization] email account for work. Do not use personal email accounts for work, and do not forward work email to a personal account.
- Check the recipients before you send, especially when the address autocompletes, and use Bcc when emailing a group of external people who should not see each other's addresses.
- Do not send personal data or confidential information by email unless it is necessary. Where it is, send it only to people who need it, and [use encryption or a password-protected file, sending the password by a different route].
- Be alert to phishing. Do not open unexpected attachments or click links in messages you were not expecting. Report suspicious messages to [role or report button].
- Confirm any request to change bank details, make an urgent payment or send sensitive information by calling the person on a number you already have, not one given in the message.
- Email is a business record. Write professionally, and remember that emails may have to be disclosed in legal proceedings or in response to a request from the person they are about.
- Do not use [Organization] email to sign up for personal services, newsletters or social media.

9. Internet and social media

- Internet access is for work. Limited personal browsing during breaks is allowed if it follows section 5.
- Do not download files or software from untrusted websites, and do not use file-sharing or torrent sites.
- Only staff authorized by [role] may post on [Organization]'s social media pages or speak for [Organization] online.
- On your personal social media, do not post confidential information, information about customers or colleagues, or photos or videos taken at work that show screens, documents, customers or security arrangements, without permission.
- If you mention that you work for [Organization], make clear your views are your own, and do not post anything that could reasonably be seen as harassment, discrimination or harmful to [Organization]'s reputation.
- Be careful about what you share publicly about your role and our systems. Criminals use job titles, org charts and photos of office equipment to plan scams.
- Report fake accounts or pages pretending to be [Organization] or our staff to [role].

10. Messaging apps, including WhatsApp

Many teams use WhatsApp and similar apps to coordinate work. They are convenient, but messages sit on personal phones, are easily forwarded and are hard to delete once sent. These

rules apply to any messaging app used for work.

- Approved messaging apps for work are [e.g. Microsoft Teams, WhatsApp for team coordination only]. [Customer communication by WhatsApp uses the [Organization] WhatsApp Business account only.]
- Do not send passwords, access codes, card or bank account numbers, TRNs, copies of ID documents, medical information or other sensitive personal data by messaging app unless [role] has approved that use.
- Keep customer personal data out of group chats. Share it through [the approved system] instead.
- Work groups are created and administered by [role or managers], with at least one manager as an admin. Members who leave the team or [Organization] are removed straight away.
- Check which group you are posting in before you send. Messages and photos posted in the wrong group can be a data breach.
- Decisions, instructions and customer requests received by message must be recorded in [the official system or email], because chats are not our record.
- Turn on two-step verification in WhatsApp (Settings, Account, Two-step verification) and set a screen lock on your phone.
- Be alert to impersonation. If a message from a "manager", "director" or "supplier" on a new number asks for money, gift cards, codes or information, confirm by calling them on the number you already have.
- Do not record calls or screenshot conversations with colleagues or customers for non-work purposes.

11. Artificial intelligence tools

Use of AI tools, including chat assistants, transcription tools and AI features built into other software, is covered by the [Organization] AI Acceptable Use Policy. In summary: use only approved tools with your work account, never enter personal data, confidential information or passwords unless that policy allows it, and check AI output before you use it.

12. Personal devices (BYOD)

[Organization] [allows / does not allow] staff to use personal devices for work. Where it is allowed:

- Register the device with [role] using the form in Appendix A before using it for work, and only use it for the work apps and accounts listed on that form.
- The device must meet the minimum requirements in Appendix A: a supported operating system with security updates installed, a screen lock, encryption, and no jailbreaking or rooting.

- [Organization] may require you to install [device management or app protection software] to keep work data in a separate, protected area. [Organization] will not access your personal photos, messages, browsing or other personal content.
- If the device is lost or stolen, or you leave [Organization], we may remotely remove work apps and data. [Where the device is fully managed, this may include a full reset; you will be told before you register it.] Keep your own backups of personal content.
- Do not save work files to personal storage, personal cloud accounts or the phone's photo gallery.
- Do not let other people use the device while it is signed in to work accounts.
- Report a lost or stolen device to [role] straight away, and within [24 hours] at the latest.
- [Organization] [does / does not] contribute to the cost of personal devices or data plans used for work: [details].

13. Remote work and public Wi-Fi

- Work from home or other locations only as agreed with your manager, using company devices or registered personal devices.
- Connect to [Organization] systems through [the VPN or approved remote access method]. Do not set up your own remote access tools.
- Avoid public Wi-Fi in cafes, hotels, airports and similar places for work. Use [the VPN] or your phone's mobile hotspot instead. Never use public Wi-Fi to access banking or finance systems.
- Your home Wi-Fi must have a strong password, and the router's default admin password must be changed.
- Position your screen so others cannot read it, and take calls where you will not be overheard. Lock your screen whenever you step away, even at home.
- Do not print work documents at home unless necessary. Bring printed personal data back to the office for secure disposal; do not throw it in household trash.
- Keep work devices connected through a surge protector, and save work regularly to [approved storage] so power cuts do not lose it.

14. Software installation

- Only install software, apps, browser extensions and plug-ins that [role] has approved. [Staff do not have admin rights to install software; request it from IT.]
- Request new software from [role] by [email or IT request system], explaining what it is for. [Role] will check its security, licensing and how it handles our data before approving it.
- Never install pirated, cracked or unlicensed software, or software from pop-up adverts or unofficial download sites.

- Do not sign up for free online services and connect them to [Organization] accounts, files or email without approval.
- Do not disable or uninstall antivirus, updates or management software.

15. Data handling and personal data

[Organization] is responsible under the Act for the personal data it holds about customers, staff and others. The Act sets data protection standards: fairness and lawfulness, purpose limitation, data minimization, accuracy, storage limitation, respect for the rights of data subjects, appropriate technical and organizational security measures, and limits on transferring personal data outside Jamaica. In practice, that means:

- Collect and use only the personal data you need for your job, and only for the purpose it was collected for.
- Access customer and staff records only when you have a work reason to. Looking up a neighbor, relative or public figure out of curiosity is not allowed.
- Keep personal data accurate, and keep it only as long as our [records retention schedule] allows.
- Store personal data only in approved systems and locations (section 16). Do not keep copies on your desktop, personal devices or personal accounts.
- Do not send personal data outside Jamaica, for example by uploading it to an unapproved overseas online service, unless [the Data Protection Officer] has approved it.
- Pass requests from people to see, correct or delete their personal data to [the Data Protection Officer] straight away so they can be answered promptly.
- Dispose of paper with personal data by [shredding or secure disposal bin], and give old devices and storage to [role] for secure wiping or destruction.

Handle information according to its category. If you are unsure, treat it as the higher category or ask [role].

Category	Examples	How to handle it
Public	Website content, published brochures, press releases	No restrictions.
Internal	Procedures, internal notices, routine meeting notes	Keep within [Organization]. Store in approved systems.
Confidential	Contracts, pricing, financial records, client files, plans	Share only with people who need it. Do not send to personal accounts or messaging groups. Encrypt when sending outside [Organization].

Category	Examples	How to handle it
Personal data	Customer and staff records, contact details, TRNs, account numbers, CVs, CCTV footage	As confidential, plus the rules above. Minimum necessary only.
Sensitive personal data	Health and medical records, biometric data, criminal records	Only staff authorized by [role]. Never by messaging app or personal email. Encrypt always.

If personal data is lost, stolen, sent to the wrong person or accessed without authority, report it straight away (section 19). The Act requires certain breaches to be reported to the Information Commissioner within 72 hours of becoming aware of them, and affected people to be told as required by the regulations, so every hour matters.

16. Removable media and cloud storage

- Store work files in [approved cloud storage, e.g. OneDrive, SharePoint or Google Drive using [Organization] accounts] or [the shared drive].
- Do not store or share work files using personal cloud accounts, personal email or file transfer websites that [role] has not approved.
- When sharing files from cloud storage, share with named people rather than "anyone with the link", and set an expiry date for external sharing where possible. Remove access when it is no longer needed.
- [USB drives and external hard drives may only be used if issued by [role] and encrypted. / USB storage is blocked on company devices.]
- Never plug in a USB drive, phone or other device you found, were sent unexpectedly or were given at an event. Hand it to [role].
- Do not copy personal or confidential data to removable media unless [role] has approved it, and delete it as soon as it is no longer needed.

17. Physical security of devices

- Lock your screen every time you leave your device, and set it to lock automatically after [5] minutes.
- Keep laptops and phones with you in public. Do not leave them visible in a vehicle; if you must leave them in a vehicle briefly, lock them out of sight before you arrive, not in the parking lot.
- Carry laptops as hand luggage when travelling.
- Lock away laptops, phones and paper files at the end of the day [in a locked drawer or cabinet], and keep desks clear of confidential papers.

- Do not leave documents on printers or photocopiers. Collect them straight away.
- Keep server, network and CCTV equipment in locked rooms or cabinets. Only authorized people may enter, and visitors must be accompanied.
- Protect equipment from power surges and outages with surge protectors and UPS units where provided, and make sure portable devices are secured or moved to safety when a storm or hurricane is expected.

18. Monitoring

[Organization] monitors its systems to keep them secure, to protect our information and customers, to meet our legal obligations and to investigate suspected breaches of this policy. We want staff to know exactly what we monitor. We monitor only the following:

What we monitor	Why	Who can see the results	How long we keep it
[e.g. Websites visited on company devices and network]	[Blocking malicious sites, investigating incidents]	[IT provider, Operations Manager]	[e.g. 90 days]
[e.g. Email for malware, phishing and data leaks]	[Security]		
[e.g. Sign-in records and device security status]	[Detecting account misuse]		
[e.g. CCTV in [locations]]	[Security of premises and staff]		

- Monitoring is carried out in a way that is necessary and proportionate to these purposes. We do not monitor personal content on registered personal devices.
- Individual email, messages or files are only looked at when there is a specific reason, such as a security incident, a legal requirement or a suspected serious breach of policy, and only with the approval of [role, e.g. the Managing Director]. Access is recorded.
- Information from monitoring is personal data. It is handled under the Act and our [data protection policy], kept securely, seen only by the people listed above and deleted when the retention period ends.
- Because work systems may be monitored as described here, avoid using them for anything you want to keep private.
- If we change what we monitor, we will update this section and tell staff before the change takes effect.

[Note for the organization: delete this note before adopting the policy. Monitoring staff raises data protection and employment-law questions. Check this section with your own legal adviser, describe only the monitoring you actually do, and consider whether a data protection impact assessment is needed before introducing new monitoring.]

19. Reporting incidents

Report to [role, email and phone number] straight away, at any time of day, if:

- a company device, a registered personal device or removable media is lost or stolen;
- you clicked a link, opened an attachment or entered a password or MFA code you think was a scam;
- you approved a sign-in prompt you did not start, or your account is doing things you did not do;
- your device behaves strangely, shows ransom or warning messages, or files are missing or renamed;
- personal or confidential information was sent to the wrong person, posted in the wrong group or accessed by someone who should not have it;
- you see someone breaking this policy or trying to get unauthorized access.
- If you think your device is infected, disconnect it from the network (turn off Wi-Fi or unplug the cable) but leave it switched on unless IT tells you otherwise.
- Do not try to investigate, delete evidence, or contact the attacker yourself.
- Reporting quickly limits the harm. You will not be penalized for reporting an honest mistake promptly. Hiding an incident is a serious breach of this policy.

[Role] will handle the incident under our [incident response plan], and the Data Protection Officer will decide whether it is a personal data breach that must be reported to the Information Commissioner.

20. Leaving the organization

When you leave [Organization], or move to a role that needs different access:

- Return all company devices, keys, access cards, security keys and removable media by your last day, using the return section of Appendix B.
- Hand over work files, passwords for shared accounts (through the password manager) and ongoing work to your manager. Do not delete work files or email.
- Do not copy, forward or take any [Organization] information, including customer lists and contacts, when you leave.
- Remove work apps, accounts and data from registered personal devices, or allow [role] to remove them remotely.

- Your duty to keep [Organization] information confidential continues after you leave.

Managers and IT complete this checklist for every leaver:

- ☐ IT notified of the leaving date at least [5 working days] in advance.
- ☐ Accounts disabled at the end of the last working day, or immediately for dismissals.
- ☐ Email forwarded to or shared with [manager] for [30] days, with an auto-reply giving an alternative contact.
- ☐ Removed from WhatsApp and other messaging groups used for work, and from social media page roles.
- ☐ Passwords changed for any shared accounts, door codes or alarm codes the person knew.
- ☐ MFA devices, security keys and remote access removed.
- ☐ Work data removed from registered personal devices.
- ☐ All equipment returned and checked against Appendix B.
- ☐ Access to third-party systems (banks, suppliers, government portals) removed or transferred.

21. Breaches of this policy

- Breaking this policy may lead to loss of access to systems or devices and to disciplinary action under our [disciplinary policy], up to and including dismissal for serious breaches.
- Some breaches, such as unauthorized access to personal data or computer systems, may also be criminal offences or breaches of the Act.
- Contractors and other third parties who break this policy may have their access removed and their contract ended.
- If you need an exception to any part of this policy, ask [role] in writing. Approved exceptions are recorded, time-limited and reviewed.

22. Review and related policies

[Role] reviews this policy every [12] months, or sooner if the law, guidance from the Information Commissioner, our systems or the way we work change.

Related policies: Password and Authentication Policy; AI Acceptable Use Policy; [Data Protection and Privacy Policy; Information Security Policy; Incident Response Plan; Records Retention Policy; Social Media Policy; Remote Work Policy; Disciplinary Policy]. [Delete any that do not apply.]

Appendix A: Personal Device (BYOD) Registration Form

Complete this form before using a personal device for [Organization] work. [Role] keeps the completed forms.

Question	Answer
Name, role and department	
Device type (phone, tablet, laptop)	
Make and model	
Operating system and version	
Phone number (for phones)	
Work apps and accounts to be used (e.g. email, Teams, WhatsApp work groups)	
Device management or app protection software installed (yes, no, not required)	
Approved by [role] and date	

Minimum requirements, checked by the staff member and [role]:

- ☐ The operating system is still supported by the manufacturer and all security updates are installed.
- ☐ A screen lock (PIN of at least [6] digits, password or biometric) is set, locking automatically after [5] minutes or less.
- ☐ The device is encrypted (on by default on current iPhones and most current Android phones; turned on for laptops).
- ☐ The device is not jailbroken or rooted.
- ☐ Apps are installed only from the official app stores.
- ☐ Find-my-device or remote locate is turned on.
- ☐ Two-step verification is turned on in WhatsApp and any other messaging app used for work.
- ☐ The staff member has read section 12 of the IT Acceptable Use Policy, including what [Organization] can and cannot see and remove.

I agree to use this device for [Organization] work in line with the IT Acceptable Use Policy, to report its loss or theft straight away, and to allow work apps and data to be removed when I leave or if the device is lost.

Staff signature	
Date	

Appendix B: Equipment Issue and Return Form

[Role] completes this form when equipment is issued and again when it is returned. Keep a copy in the staff member's file.

Staff member	Role and department	Manager

Item	Make and model	Serial or asset number	Condition when issued	Date issued	Condition when returned	Date returned
[e.g. Laptop]						
[e.g. Charger]						
[e.g. Phone]						
[e.g. Security key]						
[e.g. Access card or keys]						

On issue: I have received the equipment listed above in the condition shown. I will look after it and use it in line with the IT Acceptable Use Policy, report loss, theft or damage straight away, and return it when asked or when I leave.

	Staff member	Issued by
Name		
Signature		

	Staff member	Issued by
Date		

On return:

- ☐ All items listed above returned, or missing items noted with the reason.
- ☐ Work files saved to [approved storage] and the device checked by IT.
- ☐ Device reset or securely wiped by IT before reissue or disposal.
- ☐ Access cards and keys deactivated or recovered.

	Staff member	Received by
Name		
Signature		
Date		

Appendix C: Staff Acknowledgement

I have read and understood the [Organization] IT Acceptable Use Policy, version [1.0], including the monitoring described in section 18, and I agree to follow it. I have also read the Password and Authentication Policy and the AI Acceptable Use Policy. I understand that breaking these policies may lead to disciplinary action.

Name	
Role and department	
Signature	
Date	