Bring Your Own Device (BYOD) Policy

vStream Digital Media / ShineVR

Last updated 03/02/25

Definitions

Term	Definition
Company	means vStream Digital Media
ShineVR	means the ShineVR product developed and operated by vStream Digital Media
GDPR	means the General Data Protection Regulation
Responsible Person	means Andrés Pitt, CTO
BYOD	Bring Your Own Device - the practice of employees using their personal devices for work purposes
Personal Device	Any computing device owned by an employee including smartphones, tablets, laptops, or desktop computers
Company Data	Any data owned by or processed on behalf of vStream Digital Media or ShineVR, including emails, documents, customer data, and application data
Managed Applications	Work-related applications such as Google Workspace, Slack, and ShineVR testing applications

1. POLICY STATEMENT

vStream Digital Media recognises that employees may wish to use their personal devices for work purposes and that ShineVR application testing often occurs on personal smartphones. This Bring Your Own Device (BYOD) policy establishes security requirements and acceptable use guidelines for personal devices accessing Company systems or data.

Whilst the Company respects employee privacy and ownership of personal devices, employees who choose to use personal devices for work purposes must implement appropriate security measures to protect Company and ShineVR data. This policy balances operational flexibility with information security requirements.

2. PURPOSE

The purpose of this policy is to:

- Define security requirements for personal devices used for work purposes
- Protect Company and ShineVR data accessed from personal devices
- Clarify responsibilities for device security and management
- Establish acceptable use guidelines for personal devices
- Ensure compliance with GDPR and data protection requirements
- Protect employee privacy whilst securing Company data
- Define support limitations for personal devices

3. SCOPE

This policy applies to:

- All employees, contractors, and temporary staff of vStream Digital Media
- All personal devices used to access Company email, documents, systems, or data
- Personal smartphones used for ShineVR application testing
- Personal devices used for remote working or homeworking
- Personal devices used to access Google Workspace applications
- Personal devices used to access Slack or other Company communication platforms

This policy does not apply to:

- Company-owned devices (covered under separate IT policies)
- Devices that never access Company data or systems
- Guest devices used only for internet access at Company premises

4. PERMITTED USES OF PERSONAL DEVICES

4.1 Approved Activities

Personal devices may be used for:

- Accessing Company email via Google Workspace
- Accessing Company documents stored in Google Drive
- Using Slack for work communications
- Testing ShineVR mobile applications
- Participating in video conferences (Google Meet)
- Accessing Company calendar and contacts
- Reviewing and editing work documents
- Two-factor authentication for Company systems

4.2 Prohibited Activities

Personal devices must not be used for:

- Accessing production ShineVR databases directly
- Accessing Google Cloud Platform production infrastructure (except via authorised management interfaces)
- Storing unencrypted Company confidential information locally
- Storing passwords in unsecured files
- Bypassing Company security controls or monitoring
- Sharing Company credentials with family members or others
- Processing large volumes of customer personal data locally
- Developing code without appropriate version control and backup

4.3 ShineVR Application Testing

For employees testing ShineVR applications on personal smartphones:

- Testing should use designated test/staging environments, not production data
- Test data must be anonymised or synthetic, never real customer PII
- ShineVR test applications should be removed when testing is complete
- Any issues discovered during testing must be reported via proper channels
- Test credentials must not be shared or reused for production access

5. SECURITY REQUIREMENTS FOR PERSONAL DEVICES

All personal devices used for work purposes must meet the following mandatory security requirements:

5.1 Operating System and Software Updates

Mandatory Requirement: Devices must run current, supported operating systems with latest security updates

Specific Requirements:

- **Mobile devices (iOS/Android):**
  - Must run a version of iOS or Android still receiving security updates from manufacturer
  - Security updates must be applied within 30 days of release
  - Operating system must be updated to latest major version within 90 days of release
  - End-of-life operating systems are prohibited (e.g., iOS versions no longer supported by Apple)
- **Computers (Windows/macOS/Linux):**
  - Must run supported operating system version receiving security updates
  - Security patches must be applied within 30 days of release
  - Automatic updates should be enabled where possible
- **Application updates:**
  - All work-related applications (Google Workspace, Slack, etc.) must be kept updated
  - Updates should be applied within 14 days of availability

5.2 Anti-Malware and Security Software

Mandatory Requirement: Devices must have active, up-to-date anti-malware protection

Mobile Devices (iOS/Android):

- Install and maintain anti-malware software from reputable provider
- Ensure anti-malware definitions are updated automatically
- Run regular scans (at least weekly)

Recommended Mobile Anti-Malware Solutions:

- **Free/Low-Cost Options:**
    - **Android:** Google Play Protect (built-in), Avast Mobile Security, Bitdefender Mobile Security
    - **iOS:** Lookout Mobile Security, Avira Mobile Security, Trend Micro Mobile Security
- **Paid Options (Enhanced Protection):**
    - Norton Mobile Security
    - Kaspersky Mobile Security
    - McAfee Mobile Security

Computers (Windows/macOS/Linux):

- Install and maintain anti-malware software
- Enable real-time scanning
- Ensure automatic updates are enabled
- Run full system scans weekly

Recommended Computer Anti-Malware Solutions:

- **Free Options:**
    - Windows Defender (Windows built-in)
    - Avast Free Antivirus
    - AVG AntiVirus Free
- **Paid Options:**
    - Norton 360
    - Kaspersky Internet Security
    - Bitdefender Total Security

5.3 Device Lock and Authentication

Mandatory Requirements:

- **Screen lock:** Must be enabled with automatic timeout
    - Maximum timeout: 5 minutes for computers, 2 minutes for mobile devices
    - Immediate lock when device left unattended
- **Authentication method:**
    - Strong password/passphrase (minimum 8 characters) OR
    - Biometric authentication (fingerprint, face recognition) OR
    - PIN (minimum 6 digits)
- **Failed attempt lockout:** Enable device lockout after maximum 10 failed attempts
- **Password managers:** Recommended for managing work-related passwords

5.4 Encryption

Mandatory Requirement: Full device encryption must be enabled

Implementation:

- **iOS devices:** Encryption enabled by default when passcode is set
- **Android devices:** Enable encryption in Settings > Security (varies by device)
- **Windows computers:** Enable BitLocker full disk encryption
- **macOS computers:** Enable FileVault full disk encryption
- **Linux computers:** Use LUKS or dm-crypt for full disk encryption

Verification:

- Employees must verify encryption is active on their devices
- IT support can provide guidance on verification if needed

5.5 Network Security

Mandatory Requirements:

- **Avoid public Wi-Fi:** Do not access sensitive Company data over public Wi-Fi without VPN
- **Home network security:**
    - Home Wi-Fi must use WPA2 or WPA3 encryption (not WEP or open networks)
    - Change default router passwords
    - Keep router firmware updated
- **VPN usage:** Use Company-approved VPN when accessing Company systems over untrusted networks (if VPN provided)
- **Bluetooth:** Disable Bluetooth when not in use; never pair with unknown devices

5.6 Application Security

Mandatory Requirements:

- **Official app stores only:** Install applications only from official stores (Apple App Store, Google Play Store)
- **App permissions:** Review and limit application permissions to only what is necessary
- **Avoid jailbreaking/rooting:** Devices must not be jailbroken (iOS) or rooted (Android)
- **Work profile separation (Android):** Use Android Work Profile if available to separate work and personal data
- **Managed applications:**
    - Google Workspace applications (Gmail, Drive, Calendar)
    - Slack
    - Any Company-approved work applications
- **Prohibited applications:**
    - Applications from untrusted sources

- Applications with known security vulnerabilities
- Peer-to-peer file sharing applications
- Applications that bypass Company security controls

5.7 Data Storage and Backup

Mandatory Requirements:

- **Cloud storage preferred:** Store work documents in Google Drive, not locally on device
- **Local storage minimised:** Avoid storing Company data locally where possible
- **Encrypted local storage:** If Company data must be stored locally, use encrypted containers
- **No unencrypted backups:** Device backups must be encrypted
    - iOS: iCloud backup with encryption or encrypted iTunes backup
    - Android: Google backup with encryption or encrypted local backup
- **Removable media:** Avoid using USB drives or SD cards for Company data; if necessary, must be encrypted

5.8 Physical Security

Mandatory Requirements:

- Never leave device unattended in public places
- Use privacy screens when working in public locations
- Report lost or stolen devices immediately (within 2 hours)
- Enable "Find My Device" features (Find My iPhone, Find My Device for Android)
- Remote wipe capabilities should be enabled where possible

6. EMPLOYEE RESPONSIBILITIES

Employees using personal devices for work must:

6.1 Security Compliance

- Implement all mandatory security requirements listed in Section 5
- Maintain devices in secure condition at all times
- Report security incidents or device compromise immediately
- Report lost or stolen devices within 2 hours to CTO (andres@vstream.ie)
- Allow remote wipe of Company data if device is lost or stolen
- Remove Company data when leaving employment or ending device use for work

6.2 Software and Updates

- Keep operating systems and applications updated
- Install security updates within required timeframes

- Maintain active anti-malware protection with current definitions
- Remove or update applications that develop security vulnerabilities

6.3 Data Protection

- Store work documents in Google Drive, not locally
- Use strong authentication for all work-related accounts
- Enable two-factor authentication where required
- Never share work credentials with others
- Protect device from unauthorised access by family members or others
- Back up important work data to Google Drive
- Delete work-related data when no longer needed

6.4 Acceptable Use

- Use devices responsibly and professionally
- Comply with Company's Information Security Policy
- Comply with Company's Acceptable Use Policy (if applicable)
- Respect intellectual property and copyright
- Do not use devices for illegal activities
- Maintain professional communications when using Company accounts

6.5 Incident Reporting

Report immediately to CTO (andres@vstream.ie):

- Lost or stolen device (within 2 hours)
- Suspected malware infection
- Suspected unauthorised access to Company accounts
- Device compromise or security breach
- Inadvertent disclosure of Company data
- Any other security incident involving personal device

7. COMPANY RESPONSIBILITIES

The Company will:

7.1 Policy and Guidance

- Provide clear BYOD security requirements
- Offer guidance on implementing security measures
- Maintain list of recommended security software
- Provide training on device security best practices
- Update policy as threats and technologies evolve

7.2 Support and Assistance

- Provide guidance on security configuration (within reasonable limits)
- Assist with Google Workspace setup on personal devices
- Provide two-factor authentication support
- Offer guidance on encryption and security software
- However, note that full IT support is limited for personal devices (see Section 8)

7.3 Incident Response

- Respond to reported device security incidents
- Coordinate remote wipe if device is lost or stolen
- Investigate security breaches involving personal devices
- Revoke access to Company systems if device is compromised

7.4 Privacy Respect

- Not install monitoring software on personal devices
- Not access personal data or applications on employee devices
- Limit Company access to work-related data only
- Respect employee privacy and personal use of devices

8. COMPANY SUPPORT LIMITATIONS

8.1 Limited IT Support

The Company provides limited support for personal devices:

Supported:

- Google Workspace account setup and configuration
- Two-factor authentication enrollment
- Password resets for Company accounts
- Basic guidance on security settings
- Incident response for security breaches

Not Supported:

- Device repairs or hardware issues
- Personal application problems
- Operating system troubleshooting (beyond security guidance)
- Data recovery from personal devices
- Device performance optimisation

- Personal email or application setup

8.2 Employee Responsibility for Device Costs

Employees are responsible for:

- Purchase cost of personal devices
- Mobile data plans and costs
- Device repairs and maintenance
- Replacement costs if device is lost, stolen, or damaged
- Anti-malware software subscriptions (if using paid options)
- Device insurance (recommended)

8.3 No Company Liability for Personal Devices

The Company is not liable for:

- Damage to personal devices
- Loss or theft of personal devices
- Data loss from personal devices
- Costs associated with malware infections
- Performance issues or device problems
- Personal data loss or exposure

9. DATA MANAGEMENT AND SEPARATION

9.1 Work Data vs. Personal Data

- Work data remains Company property even when stored on personal devices
- Employees should use separate work and personal accounts where possible
- Use Google Workspace applications for work, personal applications for personal use
- Avoid mixing personal and work data in the same applications or files

9.2 Company Data Ownership

- All Company and ShineVR data remains Company property
- Company retains the right to access work-related data on personal devices if necessary
- Company retains the right to request deletion of Company data
- Employees must return or delete Company data when requested

9.3 Data Deletion Upon Separation

When employment ends or employee stops using personal device for work:

- Employee must delete all Company data from personal device
- Remove Company email accounts (Google Workspace)
- Remove Company applications (Slack, ShineVR, etc.)
- Clear browser data for Company systems
- Delete any Company documents stored locally
- IT will revoke device access to Company systems

10. REMOTE WIPE CAPABILITY

10.1 When Remote Wipe May Be Used

Company may remotely wipe work-related data from personal devices if:

- Device is lost or stolen (with employee consent)
- Device is compromised by malware or hacking
- Employee leaves Company and fails to remove Company data
- Legal or regulatory requirement to delete data
- Serious security incident requires immediate data removal

10.2 Selective Wipe vs. Full Wipe

- **Preferred:** Selective wipe of Company data only (Google Workspace accounts, Company apps)
- **Full wipe:** May be necessary in extreme circumstances (employee will be notified if possible)
- Employees are encouraged to maintain backups of personal data

10.3 Employee Consent

- Using personal device for work implies consent to selective wipe of Company data if necessary
- Employees will be notified before wipe is performed whenever possible
- Emergency situations may require immediate wipe without advance notice

10.4 Backup Recommendations

Employees should:

- Regularly back up personal data (photos, contacts, personal files)
- Use cloud backup services for personal data (iCloud, Google Photos, etc.)
- Test backups periodically to ensure they work
- Keep personal and work data separate to facilitate selective wipe

11. PRIVACY CONSIDERATIONS

11.1 Employee Privacy Protection

The Company respects employee privacy:

- No monitoring software installed on personal devices
- No access to personal applications or data
- No tracking of device location (except "Find My Device" for lost devices with consent)
- No review of personal communications or browsing history
- Access to personal device limited to work-related incident response only

11.2 Company Data Access Rights

For work-related data only, Company retains rights to:

- Access Company email and documents on personal devices if necessary
- Review logs of Company system access from personal devices
- Remotely wipe Company data if device is lost or compromised
- Investigate security incidents involving personal devices

11.3 Transparency

Company will:

- Be transparent about what data Company can access
- Notify employees if access to device is needed (except in emergency)
- Document any access to employee devices
- Respect employee privacy to maximum extent possible

12. COMPLIANCE AND MONITORING

12.1 Compliance Verification

- Employees must self-certify compliance with BYOD security requirements annually
- CTO may request evidence of compliance (e.g., screenshot showing encryption enabled)
- Spot checks may be conducted to verify security requirements are met
- Non-compliance must be remediated within 14 days of notification

12.2 Security Assessments

- Google Workspace access logs reviewed for unusual activity

- Security incidents involving personal devices tracked and analysed
- BYOD risks included in Company risk register
- Policy effectiveness reviewed annually

12.3 Enforcement

Failure to comply with BYOD security requirements may result in:

- Warning and requirement to remediate within 14 days
- Temporary suspension of access to Company systems from personal device
- Permanent revocation of BYOD privileges
- Disciplinary action up to and including termination (for serious violations)
- Liability for damages if non-compliance leads to data breach

13. SPECIAL CONSIDERATIONS

13.1 Processing Customer Personal Data

Employees must not:

- Store customer PII locally on personal devices
- Access production databases containing customer data from personal devices
- Screenshot or copy customer personal data to personal devices
- Use personal devices to process large volumes of customer data

If customer data must be accessed:

- Access only via secure web interfaces (browser-based)
- Never download customer data locally
- Clear browser cache and data after each session
- Report any inadvertent download of customer data immediately

13.2 Regulated Data (Health Data for ShineVR)

For health-related data (pain scores, clinical data):

- Access only via secure, encrypted connections
- Never store locally on personal devices
- Access only for authorised purposes
- Follow additional security measures as required
- Report any unauthorised access immediately

13.3 Development and Source Code

Developers using personal devices:

- Must use version control (Git) for all code
- Must not store source code only locally on personal device
- Must use Company repositories (GitHub, Bitbucket)
- Must follow secure coding practices on personal devices
- Must use separate development environments (not production access)

13.4 International Travel

Employees travelling internationally with personal devices containing Company data:

- Research destination country data privacy laws
- Be aware of border search and device inspection policies
- Consider using temporary "travel devices" without Company data for high-risk destinations
- Use VPN when accessing Company systems from abroad
- Report any device inspection or compromise to CTO immediately upon return

14. ACCEPTABLE USE

14.1 Prohibited Activities

Personal devices used for work must not be used for:

- Illegal activities
- Harassment or discrimination
- Sharing confidential Company information inappropriately
- Accessing inappropriate or offensive content using Company accounts
- Circumventing Company security controls
- Installing unauthorised software that compromises security
- Sharing Company credentials with others

14.2 Personal Use

- Limited personal use of work applications on personal devices is acceptable
- Personal use must not compromise device security
- Personal use must not interfere with work responsibilities
- Personal use must comply with this policy and other Company policies

15. TRAINING AND AWARENESS

15.1 BYOD Security Training

All employees using personal devices for work must complete:

- Initial BYOD security training before using device for work
- Annual refresher training
- Training on security updates and new threats
- Training covers:
    - Security requirements of this policy
    - How to implement required security measures
    - Recommended security software and configuration
    - Incident reporting procedures
    - Data protection and privacy considerations

15.2 Resources and Support

Company provides:

- List of recommended anti-malware solutions (updated quarterly)
- Step-by-step guides for enabling encryption on different devices
- Security configuration checklists
- Contact information for IT support
- Regular security awareness communications

16. EXCEPTIONS

16.1 Exception Process

Exceptions to this policy may be considered in rare circumstances:

- Must be requested in writing to CTO (andres@vstream.ie)
- Must include detailed justification for exception
- Must document compensating security controls
- Must be approved in writing by CTO
- Must be reviewed every 6 months
- Must be limited in duration

16.2 Temporary Exceptions

Short-term exceptions may be granted for:

- Device undergoing repair (temporary use of less secure device)
- Emergency work situations requiring immediate access
- Travel to locations where policy compliance is not feasible

All exceptions documented and tracked.

17. POLICY REVIEW AND UPDATES

17.1 Regular Review

This policy will be reviewed:

- **Annually** by CTO
- **When significant security threats emerge** affecting mobile devices or BYOD
- **When new device types or technologies become prevalent**
- **After security incidents** involving personal devices
- **When regulations change** affecting BYOD or data protection

17.2 Communication of Changes

- All policy updates communicated to employees via email
- Employees required to acknowledge receipt and compliance with updated policy
- Training materials updated to reflect policy changes
- Grace period provided to implement new security requirements (typically 30 days)

18. TERMINATION OF BYOD PRIVILEGES

The Company may terminate an employee's BYOD privileges:

- For serious security violations
- If device cannot meet security requirements
- If device is repeatedly compromised
- If employee fails to report incidents
- If employee refuses to allow remote wipe when necessary
- At Company's discretion for business or security reasons

Termination of BYOD privileges means:

- Immediate revocation of access to Company systems from personal device
- Requirement to use Company-provided device instead (if applicable)
- Removal of all Company data from personal device

19. ACKNOWLEDGEMENT AND AGREEMENT

By using a personal device for work purposes, employees acknowledge and agree to:

- Comply with all requirements of this BYOD policy
- Implement mandatory security measures on personal devices
- Allow Company to remotely wipe Company data if device is lost or compromised
- Accept responsibility for device security and costs
- Report security incidents and device loss immediately
- Remove Company data when employment ends or BYOD privileges are terminated
- Understand that Company has limited liability for personal device issues

20. RELATED POLICIES

This policy should be read in conjunction with:

- Information Security Policy
- Password Policy
- Encryption Policy
- Access Management Process/Procedure
- Incident Management Policy and Procedure
- Acceptable Use Policy (if applicable)
- Data Protection Policy

21. ROLES AND RESPONSIBILITIES

Role	**Responsibilities**
CTO (Responsible Person)	Policy ownership and maintenance; approve exceptions; incident response; compliance monitoring; provide security guidance
IT Support	Provide configuration guidance; support Google Workspace setup; assist with security questions; respond to incidents
Employees	Implement security requirements; maintain device security; report incidents; remove Company data upon separation; comply with all policy requirements

Role	Responsibilities
Line Managers	Ensure team members aware of policy; monitor compliance; support incident reporting; verify data removal upon separation

22. CONTACT INFORMATION

For questions about this policy or to report BYOD security incidents:

Data Protection Officer / CTO: Andrés Pitt Email: andres@vstream.ie Phone: (086) 788 6570

For Lost or Stolen Devices (Emergency): Contact CTO immediately: (086) 788 6570

BYOD Security Requirements Quick Reference Card

Mandatory Security Checklist:

- Operating system fully updated
- Anti-malware software installed and updated
- Screen lock enabled (max 5 min timeout for computers, 2 min for mobile)
- Full device encryption enabled
- Home Wi-Fi uses WPA2 or WPA3
- Store work files in Google Drive, not locally
- Never use public Wi-Fi for sensitive work
- "Find My Device" enabled
- Regular backups of personal data

Immediately Report to CTO:

- Lost or stolen device (within 2 hours)
- Suspected malware infection
- Suspected account compromise
- Any security incident

Contact: andres@vstream.ie / (086) 788 6570