

# **Travel Cyber Security Policy**

## **Bear River Charter School**

### **Purpose**

Bear River Charter School provides school-managed Google accounts and related technology systems for school business, instruction, communication, and approved educational use. Because these accounts may contain or provide access to sensitive school information, student information, employee information, and operational records, account access must be protected when users travel outside of Utah or outside of the United States.

This policy establishes expectations for the use of school-managed accounts during travel and outlines when advance notice or access restrictions may apply.

### **Scope**

This policy applies to all users of school-managed Google accounts, including employees, students, board members, contractors, and any other individuals authorized to access Bear River Charter School systems.

### **Account Monitoring and Security**

Bear River Charter School uses security monitoring tools, including services made available through UEN, to help detect unusual or potentially unauthorized account activity. These tools may identify sign-ins from unfamiliar locations, including locations outside of Utah, as suspicious.

When suspicious activity is detected, the school may temporarily restrict account access while the activity is reviewed. The review may include the Director, designated office staff, the school's IT provider, and the affected account user, as appropriate.

The purpose of this process is to protect school systems, student information, and user accounts from unauthorized access or misuse.

### **Travel Within the United States**

Users who need to access a school-managed Google account while traveling outside of Utah should notify the Director and the school's IT provider in advance whenever possible.

The notice should include:

- The dates of travel;
- The general travel location

When appropriate, the IT provider may adjust security settings for the account during the approved travel period. Any adjustment must be limited to the dates and location of the travel and must be made only as needed to support legitimate school access.

Users should continue to follow safe account practices while traveling, including avoiding public or shared devices, using secure networks when possible, and reporting any unusual account activity promptly.

## **Travel Outside the United States**

Accessing school-managed accounts from outside the United States creates additional security and data protection concerns. For that reason, users should not access school-managed Google accounts while traveling internationally unless access has been approved in advance.

International access may be approved when there is a legitimate school-related need, such as a school-sponsored trip, approved school business, or another circumstance authorized by the Director.

Before international access is approved, the user may be required to meet with the school's IT provider to review basic security expectations. These may include using only trusted devices, avoiding public Wi-Fi when possible, using multi-factor authentication when available, and promptly reporting any lost device, suspicious sign-in, or account concern.

The school may deny, limit, or revoke international account access when needed to protect school systems, student information, or school operations.

## **User Responsibilities**

All users are responsible for protecting their school-managed accounts. Users must:

- Use school accounts only for authorized school purposes;
- Keep passwords confidential;
- Avoid signing in on public or shared devices;
- Use caution when accessing accounts over public or unsecured networks;
- Report suspicious account activity, lost devices, or possible credential exposure promptly; and
- Follow any additional instructions provided by the school or IT provider before, during, or after travel.

## **Exceptions**

The Director, in consultation with the school's IT provider, may approve exceptions to this policy when there is a legitimate school need and reasonable security precautions are in place.

Exceptions should be documented, including the user, dates, location, reason for access, and any limitations or safeguards applied.

## **Violations or Security Concerns**

Approved and Adopted July 2026

Failure to follow this policy may result in temporary account restrictions, additional security review, or other action consistent with school policy and applicable law.

The school may restrict access to any school-managed account when needed to protect school systems, student information, employee information, or school operations.