

## **Faculty and Staff Technology Use Agreement**

This Acceptable Use Agreement ("Agreement") outlines the expectations for the use of school-provided technology resources (including devices, software, internet access, and online accounts) by faculty and staff ("Users") of Broadalbin-Perth CSD ("School").

### **1. Purpose:**

School technology resources are provided to support educational activities, communication, and professional development. This agreement aims to ensure responsible, ethical, and secure use of these resources by all Users.

### **2. Acceptable Use:**

Users agree to use school technology resources for legitimate school purposes only, in accordance with Board policies and administrative regulations. This includes:

- Lesson planning, instruction, and professional development.
- Communication with students, parents, colleagues, and administrators.
- Accessing educational websites, online learning platforms, and curriculum resources.
- Utilizing school-approved productivity software and collaboration tools.
- Completing job-related tasks and administrative duties.

### **3. Unacceptable Use:**

Users agree to **refrain** from the following activities while using school technology resources:

- **Illegal Activities:** Accessing or possessing illegal content like malware, viruses, or hacking tools. Engaging in cyberbullying, harassment, or threats against others. Downloading or distributing copyrighted material without permission.
- **Inappropriate Content:** Accessing or displaying websites, images, or videos that are offensive, discriminatory, or sexually suggestive.
- **Personal Use:** Excessive personal use of school technology resources like social media, online games, or unauthorized streaming. Downloading or installing unauthorized software for personal use.
- **Commercial Use:** Using school technology resources for personal business ventures or commercial purposes not approved by the School.
- **Political Activity:** Engaging in partisan political activity using school technology resources.

- **Data Security Violations:** Sharing passwords or login credentials with unauthorized individuals. Failing to report suspected security breaches or suspicious activity to the IT department.
- **Damaging Equipment:** Tampering with, damaging, or stealing school-owned technology equipment.

#### **4. User Accounts and Passwords:**

- Users are responsible for maintaining the confidentiality of their assigned username and password for school technology resources.
- Sharing passwords with others is strictly prohibited.
- Users are responsible for any activity that occurs under their account.

#### **5. Monitoring and Filtering:**

The School reserves the right to monitor User activity on school technology resources to ensure safety, responsible use, and adherence to this Agreement. This may include monitoring internet traffic, emails, and online accounts. The School may also use filtering software to block access to inappropriate websites or content.

#### **6. Data Security:**

Users are responsible for taking precautions to protect school technology resources and data from unauthorized access and security threats. This includes:

- Using strong passwords and changing them regularly.
- Not downloading suspicious files or clicking on unknown links.
- Reporting any suspected security incidents to the IT department promptly.
- Following best practices for handling sensitive student or school data

#### **7. Copyright and Intellectual Property:**

Users agree to respect copyright laws and intellectual property rights. Downloaded materials should only be used for educational purposes with proper attribution.

#### **8. Social Media:**

When using social media platforms for educational purposes, Users should maintain a professional demeanor and avoid posting confidential information about students, staff, or the school.

## 9. Consequences of Violation:

Violations of this Agreement may result in disciplinary action, including:

- Loss of access to specific technology resources or privileges.
- Requirement to attend mandatory technology use training sessions.
- Potential disciplinary action up to and including termination of employment in accordance with Board policies.

## 10. Updates to the Agreement:

The School reserves the right to modify this Agreement at any time. Notice of any changes will be communicated to Users.

## **Broadalbin-Perth CSD - Password Policy**

This policy outlines the requirements and best practices for creating and using strong passwords for all user accounts on our network. Strong passwords are crucial for protecting sensitive information and preventing unauthorized access to systems and data.

### **Password Requirements:**

- **Minimum Length:** All passwords must be at least **12 characters** long.
- **Complexity:** Passwords must include a combination of the following character types:
  - Uppercase letters (A-Z)
  - Lowercase letters (a-z)
  - Numbers (0-9)
  - Symbols (!@#\$%^&\*)
- **Restricted Characters:** Avoid using easily guessable information in your password, such as your name, birthdate, address, or common words found in a dictionary.
- **Unique Passwords:** Don't reuse the same password for multiple accounts.

**Password Best Practices:**

- **Password Managers:** Consider using a reputable password manager to generate and store strong, unique passwords for all your accounts.
- **Avoid Sharing Passwords:** Never share your passwords with anyone, including colleagues or friends.
- **Regular Password Changes:** It's recommended to change your passwords periodically, at least every **90 days**.
- **Phishing Awareness:** Be cautious of phishing attempts that try to trick you into revealing your password. Never enter your password on websites or emails that appear suspicious.
- **Multi-Factor Authentication (MFA):** Enable Multi-Factor Authentication (MFA) whenever possible. MFA adds an extra layer of security by requiring a second verification step beyond your password when logging in.

**Enforcement:**

- The IT department will enforce this password policy through automated password complexity checks during account creation and password changes. Users who violate this policy may be required to reset their password to meet the requirements and may be subject to disciplinary action depending on the severity of the violation.

**Acceptance:**

- By using school technology resources, Users acknowledge that they have read, understood, and agreed to abide by the terms of this Agreement.

**Faculty and Staff Acknowledgement**

I have read and understand the Broadalbin-Perth School Central School District's Acceptable Use Policy. I understand that if I violate the rules my Internet/network access privileges can be restricted and that I may face other disciplinary measures.

Name (printed): \_\_\_\_\_

User's Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Please sign and return this form to Human Resources.