

APPENDIX B: MUSD'S BRING YOUR OWN DEVICE POLICY

MUSD'S BRING YOUR OWN DEVICE (BYOD) POLICY

The Maricopa Unified School District's Bring Your Own Device Policy allows students to connect personal devices to the district's wireless network provided approval is granted from the principal or authorized designee, and the student's parent or legal guardian. Parents who wish to allow their child to use a personal device must have signed off on the Parent Acknowledgements and Permissions form. This policy does not extend to district owned devices.

For purposes of this policy, "device" means personally owned electronic equipment with wireless internet capability that can be used for educational purposes. This is limited to Chromebooks that are supported by Google updates.

Terms of Agreement

Access to the network is a privilege, not a right.

Use of my device while connected to the network is governed by the District's Electronic Information Services User Agreement (EISUA) policies as set forth in the Maricopa Unified School District Policy Manual, and all other district policies and regulations pertaining to the use of technology resources. I must receive signed authorization on the Parent Acknowledgements and Permissions form from my parent or legal guardian and the principal or authorized designee and before using my device on the network. I must utilize the MUSD network to connect to the internet on my device while on school grounds. This requires that I log in with my district-supplied student user ID and password. I am not to use a personal network, broadband, or other external connection to the internet. I am not permitted to have any external network services or utilities running on my device while it is connected to the MUSD network. No personal network routers, access points, switches, hubs, network printers, or any other device besides that listed in this agreement, may be connected to the network at any time.

Current antivirus software must be installed on my device and I must continue to have up to date virus definitions installed and configured. I will not store any confidential District data on my device. I am responsible for adhering to copyright, licensing laws, and guidelines for all software on my device.

I understand this approval is granted for the current school year and must be reapplied for each school year.

Districts Rights

MUSD uses filtering technology and protection measures to restrict access to inappropriate material on the network; however, it is not possible to absolutely prevent such access. Inappropriate use may result in cancellation of permission to use the network and will be followed by prompt disciplinary and/or legal action.

An agent may be installed on my device as part of my use of the network. This agent will be used to ensure the security and management of the network. Administrators, faculty and other authorized district personnel may review files and messages to maintain system integrity and ensure that users are acting responsibly.

The District's Technology Director and/or the campus department supervisor or authorized designee may revoke my privilege to use the network when I am found violating any part of this policy.

Liability

I assume all liability when installing or uninstalling any software and do so at my own risk.

I assume all liability for improperly configuring my device. I will not hold MUSD liable, under any circumstances, for theft, damage, loss of my device, or loss of data stored on my device. MUSD assumes no