Topic 1: Acceptable use of social media by employees (what can & can't employees post on their personal and professional social media accounts about work?).

Purpose: The purpose of this policy is to establish concise guidelines in relation to the acceptable usage of social media platforms by Brightington Academy Employees. This policy is intended to ensure that employees who use personal and professional social media accounts will maintain a professional manner, uphold the academy's values, and uphold confidentiality.

Scope: This policy applies to all employees of Brightington Academy, including full-time, part-time, and contracted staff. This policy is always applicable, both during and after school hours, when any form of social media activity is related to or reflects upon Brightington Academy. This policy encompasses all social media platforms, including but not limited to Facebook, X (Previously Twitter), Instagram, LinkedIn, and TikTok.

Permissions:

- Employees may post or repost content any content from approved Brightington Academy accounts to promote any events, announcements, or any work material relating to Brightington Academy.
- Employees may share forms of positive content related to the organization but must clearly state that any opinions or ideals expressed are their own and do not reflect the Academy. This must be done by including a disclaimer such as, "The views expressed here are my own and do not the represent the views of Brightington Academy.
- Employees may join and/or participate in social media groups, as long as their posts and interactions align with the academy's professional and ethical standards.
- Employees cannot engage in any form of social media activity that could result in conflicts of interest or would reflect poorly on their or the school's professional integrity.
- Employees must refrain from posting any form of confidential, proprietary, or sensitive information regarding the Academy, its client, supplies, or any of its stakeholders. This includes, but is not limited to, financial details, internal communications, and company product plans.
- Employees are prohibited from using any social media platform to harass, intimidate, or discriminate against anyone, including but not limited to fellow employees and administration, students, parents, and competitors. Any form of harassment, hate speech, discrimination, or inappropriate content is grounds for termination.

Topic 2: Acceptable use of organizational networks (what can & can't employees use organizational networks, including Internet, Web and Wi-Fi access, for? <note not focused on the computers used to access the networks, but on the network and network-accessed resources>).

Purpose: The purpose of this policy is to establish concise guidelines in relation to the usage of organizational networks by Brightington Academy Employees. This policy is intended to ensure that employees using organizational networks use it respectfully, responsibly, securely, and with the academy's mission statement, while ensuring safe network usage.

Scope: This policy applies to all employees of Brightington Academy, including full-time, part-time, and contracted staff. This policy is always applicable during school hours, and anytime an employee uses the academy's wired and wireless networks and accesses the internet on school grounds when using academy provided networks.

Permissions:

- Employees must not use academy provided networks to access, download, or distribute any form of inappropriate, offensive, or illegal content, including but not limited to pornography, hate speech, and pirated materials.
- Employees must not engage in any activities that could compromise the network security such as attempting to bypass school firewalls, installing untrusted software or applications, or using unauthorized Virtual Private Networks (VPN).
- Employees will not share network information such as passwords or other access credentials with any unauthorized individuals, including but not limited to family members, students, and guests.
- Employees are prohibited from using academy provided networks to harass, intimidate, or discriminate against anyone, including but not limited to fellow employees and administration, students, parents, and competitors. Any form of harassment, hate speech, discrimination, or inappropriate content is grounds for termination.
- Employees are prohibited from using the academy provided networks to conduct personal business, engage in political activities, or promote any personal or unauthorized personal ventures.
- Employees are prohibited from using the academy provided networks for personal streaming, gaming, or any other network intensive activity unrelated to work.
- Employees are prohibited from attempting to access administrative restricted areas of the network, including administrative systems, or confidential records (HIPPA, FERPA) without prior authorization.

Topic 3: Management of sensitive organizational information (how should employees protect, and safeguard protected classes of information (including PII, company confidential, etc.).

Purpose: The purpose of this policy is to establish concise guidelines in relation to the management and protection of sensitive information for Brightington Academy Employees. This policy is intended to ensure that employees handle and use sensitive information responsibly, securely, and in compliance with any and all ethical and legal requirements.

Scope: This policy applies to all employees of Brightington Academy, including full-time, part-time, and contracted staff. This policy is always applicable, both during and after school hours, and covers all forms of organizational sensitive information, whether it be a digital or physical format.

Permissions:

- Employees are required to use IT and academy approved storage solutions to store and transfer sensitive information such as secure server, encrypted drives, or provided cloud storage.
- Employees are required to encrypt any emails or documents containing sensitive information when transferring them digitally
- Employees are required to securely dispose of physical sensitive information by the use of a shredder or designated disposal methods.
- Employees are prohibited from storing or transferring sensitive information on a personal device or any unapproved storage method.
- Employees are required to report any suspected data breach or loss of sensitive information to the IT Department immediately.
- Employees are prohibited from sharing any sensitive information with unauthorized individuals, including but not limited to friends and family, students, or any external parties without prior authorization from Administration.
- Employees are prohibited from altering, deleting, or modifying sensitive information to ensure confidentiality and integrity of the academy's data.
- Employees are prohibited from using public or un-trusted Wi-Fi networks to access sensitive information without the utilization of a Virutal Private Network (VPN).

Topic 4: Acceptable use of personal devices on organizational networks and connecting to organizational systems (what can, and can't employees connect to the company systems, networks, and data from their personal devices and home equipment - addresses both devices brought to organizational locations, and remote work).

Purpose: The purpose of this policy is to establish concise guidelines in relation to the acceptable usage of personal devices on Brightington Academy's organizational networks and systems. This is intended to ensure that employees who are connecting to company networks and systems from personal devices do so in a safe and secure manner, in compliance with IT data protection standards.

Scope: This policy applies to all employees of Brightington Academy, including full-time, part-time, and contracted staff. This policy is always applicable, both during and after school hours, or whenever a personal device is used on-site or remotely to access the academy's network, systems, and/or data.

Permissions:

- Employees are required to only use pre-approved personal devices to connect to the academy's systems, network, and/or data.
- Employees are required to use secure Multi-Factor Authentication (MFA) devices when accessing academy systems from a personal device.
- Employees are required to access academy systems through a pre-approved Virutal Private Network (VPN) connection when accessing academy systems remotely.
- Employees are required to report any security incident involving personal or work devices to the IT department immediately.
- Employees are prohibited from accessing anything other than their work email, communication tools, and systems authorized by IT on a personal device.
- Employees are prohibited from storing or processing any form of sensitive information on personal devices without prior authorization.
- Employees are prohibited from sharing network information such as passwords or other access credentials with any unauthorized individuals, including but not limited to family members, students, and guests.
- Employees are prohibited from leaving person devices unattended while logged into academy systems or networks.
- Employees are prohibited from using public or unapproved Wi-Fi networks while accessing academy systems without a VPN.