

IT & Social Media Policy

Scope	2
IT Equipment and Guidelines	2
Acceptable Use	2
Equipment	3
Social Media.....	3
Social Media Types.....	3
Guidelines	3
<i>Respect:</i>	3
<i>Confidentiality:</i>	3
<i>Transparency:</i>	4
<i>Legality:</i>	4
<i>Responsibility:</i>	4

Purpose

The IT & Social Media Policy provides a set of guidelines for employees of Get Skilled Access (GSA), outlining your responsibilities regarding company IT equipment and email, official GSA social media channels, and public participation in social media. It is applicable in circumstances, including:

- During and outside of business hours
- On GSA premises and on private or public premises
- Via the use of GSA owned devices and via privately owned devices or facilities

This policy should be read in conjunction with GSA's other policies including but not limited to the Code of Conduct and Ethics, and the Bullying, Harassment and Discrimination Policy.



Scope

The IT & Social Media Policy applies to all employees of Get Skilled Access, including permanent, fixed term and casual employees. The policy also applies to contractors, consultants, and visitors who engage with GSA.

IT Equipment and Guidelines

IT systems are primarily a tool to be used by employees for GSA purposes relevant to your employment. Any personal use of GSA equipment and systems should not interfere with your responsibilities or the operation of the systems. GSA is the owner of all data created by employees as part of their employment and created, sent or received by users.

Acceptable Use

Acceptable Use parameters for IT systems are important to ensure the continued effective and secure operation of those systems and to protect from problems such as error, fraud, defamation, breach of copyright, unlawful discrimination, illegal activity, privacy violations and service interruptions.

As an employee of GSA, you have a number of accountabilities when it comes to Acceptable Use of IT information and equipment including (but not limited to):

- **Responsibility for all activities undertaken using your accounts** (including email), including taking reasonable steps to ensure your accounts are secure.
- **Password protection:** you must not share your password with anyone else, consistently use “strong passwords,” and should change your password regularly.
- **Data security:** you are required to protect the security of data held on mobile systems (e.g., phones, laptops, USBs and other storage devices), including maintaining reasonable virus controls where possible.
- **Appropriate behaviour:** whilst using IT & Social Media, you must consistently abide by GSA’s Code of Conduct and other policies. You must not engage in any activity that could be considered unethical and/or unlawful.
- **Confidentiality:** you must maintain confidentiality in any and all online communications as outlined in the Code of Conduct.

It is important that you report any breach or suspected breach of the Acceptable Use parameters to your supervisor as soon as possible.



Equipment

Employees of GSA must use reasonable attempts to maintain the security, integrity and usability of IT equipment and software provided by the company. All equipment including laptops, phones, screens, chargers, and accessories must be returned to your supervisor in good condition on the final day of your employment.

Social Media

Social media can be a valuable and important online networking and communication tool. Social media presents opportunities for GSA and GSA employees to extend their social reach and increase community engagement. While social media can be an effective way to interact and connect, it can also present certain risks in a workplace environment. You should assume that anything you do on social media, either via GSA's account or via a private account, can be viewed publicly, whether it was your intention or not.

Social Media Types

As a GSA employee, you are required to adhere to all GSA's policies and procedures on social media platforms including, but not limited to, Twitter, Instagram, LinkedIn, Facebook, Youtube, Tik Tok, Snapchat and any other tool or service that facilitates online interaction.

Guidelines

Respect:

Consistent with GSA's Code of Conduct, employees must maintain respect when conducting business on behalf of GSA, and when they can be identified as an employee of GSA, including when communicating via a private account. While GSA values privacy and diversity of opinion, you must not engage in any activity that can be considered in breach of the Bullying, Harassment and Discrimination Policy or that could damage the company's reputation or bring it into disrepute.

Confidentiality:

As with confidentiality in standard workplace practise, you must not share information that can be considered confidential to GSA, GSA employees and/or GSA clients online via social media or any other platform without prior consent.



Transparency:

When referencing GSA on social media, you should clearly disclose that you are an employee of GSA and you must not make any false or misleading claims, including as part of marketing and promotional activities. It is also important to monitor social media for any posts or comments that may be false or misleading and remove them as soon as possible.

Legality:

To avoid violating trademark, copyright, intellectual property rights or publicity rights, do not post images or other content without the consent of those who own or appear in the content. This includes providing proper credit for social media content (such as photographs) and ensuring you adhere to the terms and conditions of individual social media platforms, including applicable community standards.

Responsibility:

All employees of GSA are encouraged to speak about the company and share news and information via social media, however you must be sure to clearly delineate between opinion and official company response. Only specified employees may speak on behalf of GSA and all GSA social media activity should align with its specific branding guidelines.

You should avoid posting content that might contain legal conclusions, intellectual property that belongs to another organisation and defamatory or inflammatory language. If you see or become aware of inappropriate conduct on social media platforms or online more broadly, under the GSA Speak Up Procedure you should inform your supervisor as soon as possible.

When in doubt about any of the above, we ask you to consult with your manager or a trusted colleague.