Office of the Chief Information Officer Directive: IT 13.05	Published: 04/2019
Chapter: User Responsibilities	Last Review: 01/2022
Subject: **Internet Access and Acceptable Use**	

1 DIRECTIVE

1.01 Users who have access to the Internet via GNB-supplied computer systems are prohibited from:

(a) Intentionally viewing, downloading, uploading, forwarding, printing, copying or storing offensive, non-business-related information content from the Internet;

(b) Using the Internet for unauthorized personal use, productivity wasters, resource wasters, and risky activities such as accessing dating, gambling and gaming sites, participating in chat rooms, shopping and downloading streaming audio, video and other files that use excessive network bandwidth.

2 PURPOSE

2.01 The purpose of this Directive is to minimize the risks to GNB and its IT systems and networks from making Internet access available to IT users.

3 SCOPE

3.01 This directive applies to all users of GNB-supplied Internet.

4 RESPONSIBILITY

4.01 **All Internet users** are responsible to abide by the restrictions imposed by this Directive.

4.02 **Managers/Supervisors/Team Leads** may set reasonable limits and restrictions on personal use of the Internet. These limits may include prohibition when managers determine that personal use may expose GNB Information Security Policy to legal liability or exceed IT resources unduly.

4.03 **IT Technical Support** is responsible to implement system controls on Internet access through GNB systems, monitor Internet use, investigate suspected violations of Internet use, and report any Internet abuse discovered.

5 DEFINITIONS

5.01 "**Acceptable use**" refers to the rules that restrict the way in which GNB IT resources may be used.

5.02 "**Offensive material**" with respect to data available on the Internet includes content that is:

- Defamatory or libellous
- Harassing, menacing or threatening
- Obscene, pornographic or sexual in nature
- Bigoted relating to race, gender, sexual orientation or religion
- Threatening
- Containing otherwise offensive language or content
- Otherwise malicious in intent

6 RELATED DIRECTIVES

OCIO IT 8.05 – Controls for Viruses, Worms, and Malware
OCIO IT 10.07 – Email Security
OCIO IT 13.01 – System Access and Acceptable Use
OCIO IT 13.04 – Email Acceptable Use
OCIO IT 14.01 – BYOD: Acceptable Devices and Operating Systems
OCIO IT 14.02 – BYOD: System Access and Acceptable Use