GEORGIA
DEPARTMENT OF NATURAL RESOURCES

Guidelines for the Acceptable Use of Microsoft Office 365

The following are guidelines describing the acceptable use of Microsoft Office 365, communication (Skype for Business), and data storage services (OneDrive) as it applies to the Georgia Department of Natural Resources (DNR).

These guidelines provide guidance on acceptable use of Outlook (mail, tasks, and calendar), Skype for Business, and OneDrive, for the purpose of sending or receiving messages, attachments, and storage of data. It describes the standards that users are expected to observe when using these applications for email, and ensures that users are aware of the legal consequences attached to inappropriate use of the Microsoft Office 365 suite of products.

Authorized Users

DNR owns the accounts and data transmitted or stored using DNR's Office 365, subject to underlying copyrights and other intellectual property rights under applicable laws. Any use of DNR email in an unacceptable and inappropriate manner may be treated as a disciplinary offense or a matter of legal action depending on the seriousness of the offense.

Office 365 services are available for staff to conduct and communicate Agency business. Incidental personal use of email or other tools is allowed with the understanding that the primary use should be job-related, and that occasional use does not adversely impact work responsibilities or the performance of the network.

When a staff member leaves DNR by retirement, resignation or termination, the email account and contents stored will no longer be accessible to the person. The account holder is expected to clear all personal correspondence before leaving. If required, the account holder's supervisor will be given access to the account, up to a period of one month, and will notify support staff when the account can be terminated.

Acceptable Standards of Use

The main purpose for the provision of email is for the use in connection with conducting business and operational activities for DNR. The use of DNR's email address, mailbox, and data storage must be lawful and professional at all times. If users are in any doubt about what constitutes acceptable and appropriate use of email, they should seek advice and guidance from DNR's Office of Information Technology.

Unlawful Use of Email and Data Storage

Unlawful use of DNR's email addresses, mailboxes, and data storage may lead to criminal or civil legal action being taken against the individual users. Where there is evidence of a criminal offense, the issue will be reported to the police for them to take appropriate action. DNR will co-operate with the police and other appropriate external agencies in the investigation of any alleged offenses.

Unacceptable uses of email include, but are not limited to:

- Storage and transmission of materials that infringes on copyright laws, including intellectual property rights;
- Using email for any purpose that violates federal or state laws;
- Storage of data and using email for conducting personal business;

- Storage of data and sending or forwarding e-mails that are libelous, abusive, defamatory, derogatory, threatening, offensive, or contain obscene or indecent materials;
- Unauthorized transmission of confidential material concerning the activities of DNR;
- Creation or transmission of anonymous email messages, or using someone else's identity or password;
- Creation or transmission of material that is designed to or likely to cause annoyance, harassment, inconvenience, or needless anxiety to the recipients;
- Providing unauthorized use of DNR Office 365 and Skype for Business to any third party;
- Deliberate storage and transmission of unsolicited commercial or advertising material, chain letters, spam mail, or other junk mail of any kind;
- Storage of data and email activities that can corrupt other users' information or cause network interruptions, such as unauthorized broadcasting or mass mailings.

Preventing the Spread of Malicious Software (Viruses)

Users of DNR Information Technology must take all reasonable steps to prevent the receipt and transmission of malicious software by email such as computer viruses. In particular, users:

- Must not transmit any file attachments that they know to be infected with a virus;
- Must ensure that an effective anti-virus is operating on any computer which they use to access Agency IT;
- Must not open email file attachments from unsolicited or untrusted sources;
- Must not forward any suspicious emails, containing possible malicious links, to anyone else in DNR.

Spam Mail

"Spam" can be defined as "the mass electronic distribution of unsolicited email to individual email accounts".

An Anti-Spam filter has been installed on the DNR email gateway server to protect DNR from spam mail.

All incoming emails will be checked by the Spam Filter. Any suspected spam mail will be moved to the Spam Server and a notification sent to the recipient user. The recipient has the option to review or download the suspected spam email. The recipient must be responsible to blacklist the sender of any spam mail, and forward the spam only to junk@office365.microsoft.com without forwarding spam or copying spam to anyone else in DNR.

Mass Mailings

Mass electronic mailings are permitted only for official communication to DNR staff and outside entities and only with specific authorization by the account holder's supervisor. Other than the above, users may not send mass emails without prior approval for distribution to staff or external entities, or both.

Responsibilities of Office 365 Users

All Office 365 users must familiarize themselves with the contents of these guidelines in using **Outlook, OneDrive**, and **Skype for Business**. Failure to comply with the policy may lead to serious consequences, which include DNR taking necessary disciplinary action or legal action (or both) depending on the seriousness of the matter.

Email

Every staff member and those working under the guidance of DNR will be provided with DNR official email addresses. The formal email address for all communication among members of DNR is: **@dnr.ga.gov**.

Individual users are expected to assume full responsibility and accountability for their actions and mailbox when using DNR's Office 365. The use of Office 365 by individuals at DNR assumes and implies compliance with this policy, without exception, and every user of email has a duty to ensure they practice appropriate and proper use. Every email user must understand their responsibilities in this regard.

Official Email Correspondence

All official communication among staff members (including part-time, full-time, and contract employees, interns, etc.) will be via the official email address, NO EXCEPTIONS! DNR staff is expected to check email on a frequent and regular basis in order to stay current with organizational communications, recognizing that certain communications may be time-critical.

It is recommended for email to be checked daily, but at a minimum, twice per week. All staff may also use Skype for Business as a communication tool. A free Skype for Business app and OneDrive app are available for mobile devices. The OneDrive client can be installed on a computer from Office 365.

Useful Email Practices

DNR considers email as an important means of communication among its community and to external parties. Below are some useful practices on email usage:

- Do not send large files as attachments. Whenever possible, share your large files by using OneDrive.
- Read all email messages regularly and delete unwanted messages to maintain adequate storage in your mailbox.
- Activate the Auto-Reply function when you are away from the office for a period of time.
- Do not send a "REPLY ALL" if you only need to respond to the sender or selected persons.
- Be responsible and courteous in your email correspondence as the message can easily be forwarded beyond the initial circle of recipients.

OneDrive

OneDrive is a convenient cloud-based storage for your work-related files. Use OneDrive to create a central place to access documents and business information from virtually anywhere. There are security practices that still must be followed to ensure OneDrive is being used properly.

DNR has established three types of data: **Confidential, Sensitive**, and **Unclassified**.

Confidential Data

- Data that, if accessed by unauthorized entities, could cause personal or institutional financial loss or constitute a violation of statute, act or law.
- Must NOT be stored in OneDrive and should remain on FileShares or Local Drives.

Sensitive Data

- Data or other information generally used internally at DNR or with its authorized partners. If released to unauthorized individuals, it would not result in any financial loss or legal compliance issues but would negatively impact the privacy of the individuals named or the integrity or reputation of DNR.
- Sensitive data can be stored and shared in OneDrive, but must be stored and shared in a secure manner.

Unclassified Data

- Data or other information that does not meet the criteria as Confidential or Sensitive.

- The Unclassified Data classification does not imply that the data does not need to be properly managed.
- May be subject to open records requests.
- Unclassified data can be stored and shared in OneDrive, but must be stored and shared in a secure manner.

Useful OneDrive Practices

- Use folders to share groups of files with others online.
- Share files with specific individuals, never with "everyone" or the "public".
- Be careful sending links to shared folders because they can often be forwarded to others to whom you did not provide access.
- Remember that, once a file is shared with someone, and they download it to their device, they can share it with others.
- Use File Syncing Sparingly. (Use of File Sync is not recommended in most cases due to Security Issues.)

Skype for Business

Skype for Business (also known as Lync) provides chat and instant messaging with individuals or groups, video conferencing and desktop sharing.

- Skype for Business is part of the Office 2013 suite of products, available through a download from users' Office 365 accounts. Therefore, do not try to install your own copy of Skype on your computer.
- Ensure your computer is receiving appropriate GETS-provided software patches and upgrades to reduce the risk of malware from unauthorized, third party installers.
- Know who you're authorizing. Don't hesitate to block users who make unwanted contact. Keep user profiles up-to-date. Remember that everything in user profiles (except email addresses) can be seen by others.
- Always authenticate third parties before discussing any confidential business or sensitive personal information.
- Remember that, although Skype takes care to protect communications from unwanted disclosure, there is a remote possibility that your computer, or that of your contact, could have been hacked or compromised.

Disclaimer

DNR senior staff may, at its discretion, apply automatic message monitoring, filtering, and deny transmission of messages with content that is unacceptable in the terms of these guidelines. Violations of these guidelines will be handled consistent with DNR disciplinary procedures. DNR may temporarily suspend, block or restrict access to information and network resources when it reasonably appears necessary to do so in order to protect the integrity and security of DNR resources or to protect DNR from liability.