Griffith UNIVERSITY
Queensland, Australia

SMSGLOBAL BEST PRACTICE GUIDE

13 December 2022

Best practice for sending SMS to staff and students

Overview

1. Using SMS for an approved purpose
2. Practice strong cybersecurity hygiene
3. Data governance of contact lists

What are the approved uses for SMS?

The University does not use SMS for general advertisements of campus-based services or events.

The guiding principle from the Student Communication Policy is that SMS supplements electronic and paper-based communications in the following ways:

- **Emergency notices** – notify affected students of an emergency on campus, public health outbreaks or safety risks
- **Notices of changes and cancellations** – notify affected students when classes have been moved or cancelled or a change to exam venue/timetable has occurred
- **Reminders** – notify students of administrative deadlines including enrolments, graduation, assessment deadlines including submission and collection of assessment items and matters to which the student needs to attend in relation to enrolment, examination and graduation
- **Intervention** – advise students of their failure to attend an appointment with an academic advisor, or other support service, and failure to submit assessment
- **Notices of academic performance** – notify students of final grades, academic standing status and GPA
- **Service issues** – notify affected students of service outages and facility shutdowns along with timelines for when the services are likely to return to use.

Communication principles to follow

SMS use is guided by the following principles:

- **Just in time** – messages are to be sent no more than 48 hours before the action or activity affecting the student
- **Relevant** – information within the message is to be directly related to the student or their studies
- **Unambiguous** – the message must clearly state either the action (if any) that the student is required to undertake or how the information affects the student
- **Authoritative** – messages are to be sent only by those with the authority to do so and to contain a University email address for the student to contact relevant personnel for more information
- **Limited** – the number of messages received by a student within a week should not exceed five and the information able to be conveyed clearly within the 160-character limit of a text message.

SMS usage and communication principles for staff

The Student Communication Policy is also the basis for communicating to our staff via SMS. Approved uses include emergency notices, notices of changes and cancellations, critical compliance reminders and critical service issues affecting the ability of staff to be on-campus.

1. Practice strong cybersecurity hygiene

Complete your Cyber Security Essentials training

All users are expected to have completed their required Cyber Security Essentials training before applying for a new account and to keep their annual training up to date.

Cyber Security Essentials Training

Use a strong and unique passphrase to secure your account

Passwords and passphrases are the first line of defence to protect your information. They should be long, memorable and used only for this service. Griffith passwords and passphrases should never be reused for non-Griffith services. Shared accounts and passwords among teams are also no longer permitted.

If you have trouble generating strong passwords or passphrases or remembering them, use the free Griffith Password Manager available to all staff.

How to create a strong password
Griffith Password Manager–Powered by LastPass

Set up 2-factor authentication to secure your account

All accounts created will have 2-factor authentication linked to your mobile. All users must use 2-factor authentication for their accounts to add an extra layer of security. When enabled, you will be asked to enter a one-time password sent to the mobile phone registered on the account every time you attempt to log in.

If your account does not have 2-factor enabled you must set this up manually as part of your responsibility for using this service. You can be audited and lose access for not following this direction. Our Griffith Single Sign-On system is not currently integrated with the platform.

Enable 2FA (2-factor authentication for SMSGlobal logon)

Keep your devices up to date

System updates not only provide new features, but it also protects your data against vulnerabilities by patching security flaws and fixing bugs.

Mobile device and computer security

Report security incidents immediately

Report a phishing incident, password compromise, ransomware or other suspicious activity to IT immediately.

Incident reporting

2. Data governance

Information stored, accessed and disposed of at Griffith University is subject to the Information Security Classification Framework and data handling controls.

Protecting your data

Ransomware attacks target your data making it inaccessible. It is important to back up your data to stay cyber safe.

Automatic data stored on the cloud

Any data stored in SharePoint or OneDrive is automatically stored in the cloud. However, it is recommended that you keep a separate backup of important data you are working on. This prevents issues from loss of access due to an internet/service outage or a personal OneDrive becoming inaccessible if a staff member leaves Griffith University.

Keep copies

Keep a copy of important information in an additional location to your primary cloud location. The contact lists that SMSGlobal requires is also governed by the Information Security Classification Framework, limiting alternative back up locations.

Information management of Official (Internal) data—staff contact lists

SMSGlobal requires the use of staff phone numbers retrieved from PeopleSoft to send messages.

This data is classified as **Official (Internal) information** which has a restricted audience, and access must only be authorised based on academic, research or business need. There are also approved applications and services for managing and storing contact lists for use among teams.

Approved applications and services for Official (Internal) data

Document management

- SharePoint Online
- Microsoft Teams

File storage

- OneDrive for Business
- Shared Network Drive

Communication and collaboration about contact lists

- Outlook
- Microsoft Teams

Information management of sensitive data—student contact lists

SMSGlobal requires the use of student phone numbers retrieved from PeopleSoft to send messages.

This data is classified as **sensitive information** which has a restricted audience, and access must only be authorised based on academic, research or business need. There are also approved applications and services for managing and storing contact lists for use among teams.

Approved applications and services for sensitive data

Document management

- SharePoint Online*
- Microsoft Teams*

*Cannot be managed with public teams.

File storage

- OneDrive for Business*
- Shared Network Drive

Communication and collaboration about contact lists

- Outlook
- Microsoft Teams

Disposing of contact lists in SMSGlobal within 24 hours

Contact list management and storage should be limited to the above approved applications and services to avoid potential data breaches.

Immediately following the sending of your SMS to a staff or student contact list, we recommend deleting that list as soon as it is practical, if there is no ongoing requirement for it on SMSGlobal (e.g. automated responses, emergency communication exceptions).

Reporting within the platform is extremely limited, only showing whether an SMS was delivered or bounced. Making long term storage of most contact lists for data tracking and trend analysis unnecessary. For more nuanced tracking, you can use trackable short URL links from services like bit.ly.

Other resources

Cyber security at home
Phishing and other scams
Data protection
Be cyber safe when travelling