information
management & security

Gloucestershire
COUNTY COUNCIL

Gloucestershire County Council
Communicating via non-GCC approved methods in Emergencies

In emergency situations you may be required to communicate with your colleagues and / or service users when a GCC approved method isn't available. Talk to your manager about what has been agreed within your service, as there are risks that must be managed.

By following the below points, you can ensure that you protect yourself, our service users, the information you are discussing and Gloucestershire County Council.

Try to use GCC devices and approved software wherever possible. However, it is recognised that this is not always possible in an emergency situation, alternative methods you could use include, but are not limited to: WhatsApp, Messenger, Zoom, text messaging.

When communicating with service users:

- Make it clear to people the channel may not be secure and they should only share limited data;
- Do not discuss cases in detail, you must minimise the amount of personal data you discuss, and anonymise where you can;
- If you do need to discuss special category data or sensitive information this must still be sent via GCC approved routes, such as Egress email;
- Any decisions or actions must still be recorded on the relevant system on that individual's case file;
- Once an outcome has been decided and uploaded, delete the conversation from the device;
- Be aware that not all service users will want or be able to communicate this way, so keep the contact to a minimum or offer alternatives;
- Use a secure method of communication. WhatsApp, for example, comes with encryption'
- Ensure you install the latest updates for software or apps;
- Do not have open conversations on social media, such as Facebook, Twitter or Instagram, as these messages will become public and you will lose control over what happens to them.

When communicating with internal staff:
If colleagues do not have access to a laptop and/or Jabber you may need to use other methods to keep in touch with them in an emergency.

- Make it clear if a channel is for social or business discussions;
- Make it clear to people the channel may not be secure and they should only share limited data;
- Keep the messages to non-sensitive business and key messages between the team;

- Always limit personal data that is discussed, do not discuss the detail of individual cases;
- Make sure the you are still including the staff that do not use these methods to communicate the messages to them;
- Make sure these conversations are NOT set to 'back up'. Once any actions and decisions taken have been recorded in a GCC system, delete the conversation from the device.

It is the user's responsibility to:

- Ensure they read and understand this guidance;
- Report any misuse of communications. Details of how to do this are provided on the Reporting and investigating a security breach Staffnet page

Related Policies

- Code of Conduct for Employees.
- ICT Equipment Policy
- Information Protection and Handling Policy
- Information/IT Access Policy
- Data Protection Policy
- Software Management Policy
- Social Media Policy
- Password Policy

The above policies are available at Information Management and Security Policies