The Highland Council

Staff Messaging Policy

Summary

In an emergency situation, the Council needs to be able to quickly and accurately contact staff and Elected Members to warn, inform and instruct, as appropriate.

Such a situation could arise at any time and out with, as well as during, working hours. The scope of the policy also needs to include the ability to reach those staff who do not have Council email or mobile phone accounts.

The policy details how communications would be undertaken, the authority for instigating the communications and the ownership of data and systems to ensure that contact information is kept up to date.

These mechanisms are in addition to the usual methods and channels of communicating with the public in emergency situations.

For multi-agency emergency situations, the Regional (or Local) Resilience Partnership (RRP) may be convened and warning and informing will be agreed and authorised by the Police who have overall authority for Warning and Informing, particularly in the case of Terrorism or potential Criminal circumstances. (see RRP Major Incident Communications Strategy)

1. Policy

1.1 The purpose of the Staff Messaging policy is to ensure that in an emergency situation the Chief Officer in charge (i.e. Chief Executive, Duty Director) can quickly and accurately contact specific groups of staff, or all staff, as well as Elected Members.

1.2 The purpose of this communication will vary and depend on the nature of the emergency, but will generally be to warn and inform and, when required, to deploy and instruct Council resources to deal with the situation.

1.3 It is envisaged that this policy will only be used during Emergency situations when it is essential that the Council contacts all its staff or specific groups of staff, and will be part of the process by which the Council exercises its duty of care towards its staff. For example:

- A fire, flood, or similar incident in a Council building
- Severe weather incident
- A Chemical, Biological, Radiological or Nuclear (CBRN) incident
- Any serious crime or terrorism incidents e.g. marauding firearms
- Move to a Critical threat level

- A direct threat to Highland Council employees or to public sector workers

In the event of such emergency scenarios, it is highly likely that the multi-agency resilience groups would be convened to manage the response and the communication of warning and informing. The Police have the lead responsibility for warning and informing the public for most major incident events under the Civil Contingency Act.

1.4 The direct channels of communication available to the Council are: Telephone, Email, SMS Messaging (via CRM System) and Social Media. The data being used under this policy will include some personal data which must be handled in accordance with the principles of the Data Protection Act.

1.5 **Council email groups** which can be used are as follows:

- **All Staff** - to reach c. 6000 staff who have digital access
- **Members List** – All members

The All Staff council email group does not reach High Life Highland (HLH) staff and it is recommended that the Chief Executive and Communications Manager of HLH should be copied into any emergency communication.

1.6 **Personal Email**: The Council currently holds some personal email addresses for around 30% of staff for the purpose of accessing their on-line payslips. Under this policy, staff may be asked to opt to provide personal email addresses to be held within Resource Link, for the purpose of creating an **Emergency Email Group** that could be used to message staff in extraordinary emergency situations.

1.7 **SMS messaging**: The Council can create contact groups and issue bulk SMS messages via the CRM system.

The Council will create and maintain a database of telephone contact numbers that can be used to undertake group SMS messaging. A group of **all Council mobile numbers** will be created.

1.8 Under this policy, all staff may be requested to provide a personal telephone number on which they can be contacted. These would be held on Resource Link. A report would be produced of all personal contact numbers held within Resource Link, and used to create an **Emergency SMS Group** that can be used to message all staff on personal mobiles in emergency situations. (This option would require considerable resourcing.)

In order to comply with Data Protection legislation, staff would be required to opt to provide this information for the express purposes described in this policy.

If staff choose not to provide personal data for this reason, they may not receive emergency communications. There is, however, no guarantee that

emergency communication would be sent to staff in the event of an emergency as this would depend on various factors.

1.9 There is also an **Emergency Staff Directory**, which is updated on a regular basis. This contact list is included in the Duty Director's Handbook and updates emailed to Directors and Senior Managers. The digital file should be stored on council laptops for quick access. These phone numbers will be stored in the CRM system for emergency communication via SMS.

1.10 The Council has a closed **Facebook Staff Group** which is used just for staff and currently has c.700 followers. Facebook can therefore also be used in conjunction with group email and SMS messaging.

2. Messaging System

2.1 In addition to existing Council Email Groups, messaging databases would be structured to allow the following levels of messaging described above:

- Emergency Staff Directory (SMS)
- All Council Mobiles (Staff and Elected Members) (SMS)
- Emergency SMS Group – All personal telephone contacts if staff opt in for this purpose

2.2 In an emergency situation the Chief Officer in charge will instruct the use of Messaging Systems as required. No messaging would take place unless authorised by the Chief Officer.

3. Messaging Systems (content and management)

3.1 Email and SMS Groups to be created and maintained by the Digital Service Team.

3.2 The Head of People & Transformation will ensure that monthly reports are generated from the Resource Link System, in line with permissions for using the data held, and provided to the Digital Services Manager. The Digital Service Manager will be responsible for ensuring the email and SMS Groups are updated monthly and for providing access to the Chief Officer in an Emergency situation.

For new staff, explicit permission must be sought for the holding and use of any data requested.

3.3 The Key staff contact list for emergencies will be maintained and made available to the Digital Service Team by the Resilience Team.

3.4 Social Media will continue to be managed by the Corporate Communications Team. The Digital Team, Ward managers and Directors will have access to

post messages on the Staff Facebook page and Twitter.

4. Data Protection

4.1 The Council has the right to use Council email and mobile phone accounts to contact staff regarding work related matters.

The Data Protection Registry describes, in very general terms, how the Highland Council processes and uses the personal data it holds. https://ico.org.uk/ESDWebPages/Entry/Z5442561

4.2 There may be emergency circumstances in which the Council will need to contact as many staff as possible. It is permissible to use personal contact details if it is in the 'vital interests of the data subject' – Data Protection Act Schedule 2(4). Phone numbers may be stored by third parties for the purpose of sending messages, but names will not be stored.

4.3 Express permission is required from staff to contact them using personal data in any other circumstances from those described in the Data Protection Register or under Schedule 2 (4) of the Data Protection Act. Staff consent will be requested to use information held or supplied for this purpose and held within Resource Link.

4.4 Message authorisers need to be aware of:

- the principles of the Data Protection Act 1998 and the Council's guidance relating to security measures for safeguarding personal data.

5. Emergencies

5.1 Scope

Council email, mobile phones and radios may be used for the purpose of urgent information or instruction in an emergency situation as part of our routine contact procedures.

SMS Messages, emails or phone calls may be used to contact the Emergency Directory of staff who have given specific permission for the use of their details for emergency purposes.

SMS Messages or emails to **all staff** using their personal contact details may be used where content is deemed to be urgent, essential to safety and in the vital interests of staff under the Data Protection Act.

5.2 Appropriateness

SMS text messages are the most efficient way of delivering an urgent message to a large group. It should be noted that there is no guarantee that text messages will be delivered promptly, or at all, by the mobile phone

networks. Email is a less reliable form of urgent notification. Not everyone has ready access to, or notifications for personal emails on their phone.

Simultaneous, multiple approaches are essential to disseminate urgent information. Text messages should be supplemented by other means of communication, such as emails, messages issued via Facebook or Twitter or information posted on the Council website, and use of radio broadcast may be used to ensure that a message is widely received.

Mass texts or emails are not appropriate for any confidential or sensitive information.

Urgent messages should contain only warning and informing information. Staff off duty and not formally “on call” cannot be compelled to take action, carry out a duty or report to work.

5.3 Authorisation

The Chief Officer will consider if an urgent message should be sent and to which groups. This will usually be in liaison with a team of managers managing the crisis or as part of Local Resilience Partnership decision-making. During a multi-agency emergency situation, authorisation may be required from the Police to issue an alert or warning. This is particularly the case where Terrorism or criminality is a factor. Refer to the RRP Major Incident Communication Strategy for further information.

Authorisation will be given for a message only if:

- it is considered that it is urgent and necessary to get the message to a significant number of the recipients as soon as possible;
- the purpose is compelling and immediate;
- the content is both appropriate and factually correct;
- the message cannot wait for routine channels - work-hours emails and cascade communication
- the message format meets the guidelines
- Authorisation is given by the Police if the emergency involves Terrorism or criminality

5.4 There is a cost associated with SMS messaging.

5.5 Guidance on how to use the SMS messaging system will be included in the Duty Director’s handbook. Training will be provided by Digital Services.

6. Format of Message

6.1 Messages should be no longer than 160 characters and should address the member or staff member directly, i.e. as 'you'. They should include essential

points of information and action, and should avoid 'text speak', e.g. write 'you', not 'u'.

6.2 All messages must start with the words 'Council Alert:' so that the recipients of the text can see that it is an official message from the Council requiring their attention.

6.3 Subject line of emails must clearly indicate what the message concerns. E.g. “Council Alert: Chemical release”

6.4 Urgent messages will usually generate numerous questions. The SMS texting system will not be configured to allow the recipient to respond. Messages should include where to get further more detailed information e.g. intranet or website (include hyper link where possible) and/or helpline number.

A helpline number is recommended to manage resulting questions and provide additional information. The Service Centre may be used or a separate number with a pre-recorded message.

6.5 Content

Effective alerts and warnings are those that result in staff or members of the public taking recommended actions to protect themselves. To help ensure that messages are effective, they must be issued in a timely manner and should include the following components:

• Specific hazard: What hazard is threatening? What are the potential risks for the community?

• Location: Where will the impacts occur? Describe the location so those without local knowledge can understand their risk.

• Timeframes: When will it arrive at various locations? How long will the impacts last?

• Warning source: Who is issuing the warning? Identify an official source with public credibility.

• Magnitude: What impact is expected and how bad is it likely to get?

• Likelihood: How probable is occurrence of the impact?

• Protective behaviour: What protective actions should people take and when? If evacuation is called for, where should people go and what should they take with them?

7. Contact Details

7.1 Staff contact details are recorded in Resource Link. All staff will be regularly

asked to update their Contact and Emergency details on My View.

7.2 The home page of My View will contain a paragraph on how the personal and contact details may be used. Proposed wording as follows:

Personal data of employees is covered by the Data Protection Act 1998. The way in which it can be processed is covered in the Data Protection Registry.

Contact details may be used to contact you for the purpose of employment or pay related matters, or to warn and inform you in an urgent emergency situation. Your emergency contact may be contacted in the event of an emergency requiring notification of next of kin.

Staff will be asked to tick a box to agree to their personal contact details being used to contact them in an emergency situation.

An email will be sent to all staff to advise them that they will be prompted to update their details the next time they log in to My View.

7.3 For staff who do not have access to My View, paper processes must be available for providing personal contact details, for agreeing the use of the details and for updating these details on council systems.