STRICTLY PRIVATE AND CONFIDENTIAL

Dear <FIELD>

THIS IS NOT A CIRCULAR:
Notice of cyber security incident in Ards and North Down Borough Council

It is with regret that I write to inform you of some important information that has recently come to light. The Council has discovered that it was the unwitting target of an unlawful 'phishing attack' from an external source.

We are aware that this particular attack has led to some emails from our system being forwarded to an external email address. Our investigation is continuing and, whilst the full extent of the breach has not yet been concluded, we are writing to inform you that some of your personal data, which we hold, may have been exposed to a potential unauthorised use by an external party.

We would like to make you aware of the steps we are taking to deal with this matter. Firstly, we are undertaking an in-depth investigation internally. We have dedicated substantial resources to understanding what has happened; how it happened; and what information has been stolen. Secondly, we have fully notified the Information Commissioner's Office (the 'ICO') of the incident and have reported the issue to the PSNI, with whom we remain in constant contact. We have also instructed independent IT security experts to assist in our investigation. We should add that the ICO has indicated that it is entirely happy with the procedures we have adopted in order to resolve this unwanted situation.

We would also like to assure you that the necessary steps have been taken in order to prevent any further breach from this unlawful enterprise. We are hopeful that the PSNI will be able to bring the perpetrator(s) to justice, although this aspect is a matter entirely for them.

- We regret to have to inform you that we believe the following personal information about you may have been unlawfully accessed or affected by this data security incident from our email system:

- **Your <FIELD – passport/ personal/ business bank account details were accessed/ your email address/ your mobile phone number/ your home address etc were/was accessed/** however no other details/information were accessed.

We are of course extremely sorry that this has happened and appreciate it will be of considerable concern to you. We would encourage you to take steps to ensure your computer technology (including your mobile devices) is as safe as it can be and to remain vigilant as to any unwanted contact from external sources. We have outlined some steps you may take in the enclosed leaflet, based on guidance from the ICO.

What this means for you
Whilst we have no evidence that personal information of any nature has been misused, we would advise you that, based on our investigation to date and considering the type of information or data potentially breached, you may have experienced or potentially could experience some of the following consequences:

- Imposter e-mails/ letters impersonating your bank
- Scamming emails
- Phishing emails
- Unsolicited phone calls attempting to scam you
- Potential identity theft

We appreciate you may want to discuss the content of this letter with us and if that would be helpful to you, please contact –028 9127 8079. This phone line will be operational from Monday 1st March to Friday 5th March 2021 between 10am and 4pm. We are also contactable via the following email address datasupport@ardsandnorthdown.gov.uk

For your information we will be publishing a general statement about this cyber incident on our website at www.ardsandnorthdown.gov.uk

Your privacy is of paramount concern to us. We deeply regret this criminal incursion into your personal data. We are taking significant actions to minimise the potential for further data security incidents such as the present one. These include:

- Reviewing all our IT security systems and policies to ensure they are up to date and configured as per industry best practice.
- Continued education of our staff on the importance of good IT security practices.
- Working closely and consistently with external partners to ensure we are responsive to any new external threats.

Once again, we are very sorry that your personal data has been compromised in this way. The Council takes the safety and security of our customers' and partners' information very seriously. We will continue to take every action available to us to protect the organisation and all those with whom we are working against any future attacks.

Yours sincerely,

– Ards and North Down Borough Council

CC FAQ Leaflet

FAQs - What you should do if your personal data has been exposed to potential unauthorised use by an external party.

The ICO would recommend you take the following actions as soon as possible to further protect yourself from additional risks associated with this incident:

Change all affected passwords
If you find out your details have been stolen in a data breach, change your password immediately. The same goes for any other accounts using the same password. Always use strong and unique passwords and set up two-factor authentication if you can.

Check your bank account
Log into online banking and check you recognise all payments. If any seem unfamiliar, or you think someone might have unauthorised access to your account, contact your bank. Also, ask them to set up any alert features they offer. These can usually tell you when a large payment has gone through or if you're in your overdraft, helping to protect you from fraud.

Check your credit report
Checking your credit report can help you identify any unusual activity, such as new accounts, new personal information or searches on your account. If you would like to keep a closer eye on your credit score, you can also get a free Experian Credit Score, which will be updated once every 30 days when you sign in.

Beware phishing scams
Criminals may try to trick people into revealing their information following a data breach. Remember that no bank or any other genuine organisation will ask you to reveal your PIN or banking password in full. These scams can come in the form of phone calls or emails and are usually unsolicited. Phishing messages tend to be from suspicious email addresses, from a service you didn't sign up for or have unusual attachments. If you suspect it's phishing, delete it and report it to the relevant organisation.

Stay safe online
Three key tips to stay safe online are listed below.

- Do not open emails or attachments if you have any questions on the source.
- Make sure you know who you are dealing with before disclosing any personal information online.
- Always check links before clicking on them – you can do this by hovering over the link to see whether the source is recognisable. Do not click any link if you are unsure.

The ICO (www.ico.org.uk) and National Cyber Security Centre (www.ncsc.gov.uk) have useful information on their websites relating to phishing.

Please note that the Council will never contact you unprompted to ask for your account details or security information, and we will never ask you to disclose or change your passwords – nor should any other organisation.