HALE PARISH COUNCIL
OF THE HALTON BOROUGH IN THE COUNTY OF CHESHIRE

MINUTES OF EXTRA-ORDINARY MEETING OF HALE PARISH COUNCIL HELD ON TUESDAY 3 MARCH 2020 AT 4PM IN HALE VILLAGE HALL. MEETING COMMENCED AT 4.27PM.

Present: Cllr Mitchell, Cllr Cleary, Cllr Spargo, Cllr Wright, Cllr Trevaskis, Cllr Williams and Cllr Healey

1. Apologies were received from Cllr Hunter, Cllr Anderson, and Cllr Kierman.
2. Cllr Mitchell declared an interest in Items 4 , 5 and 6.
3. **The Council resolved to exclude the public and press under the Public Bodies (Admission to Meetings Act) 1960 on the grounds of the confidential nature of the business to be transacted.**
4. The Council considered a recent GDPR breach.

Members were advised that the Council had to make a decision that was considered "reasonable in the circumstances". As such, the Council followed the guidance as noted in the ICO's Code of Practice.

It was explained to members that the ICO's website affirms "GDPR requires any organisation to record all breaches, regardless of whether or not they need to be reported to the ICO".

It was confirmed that this breach had been recorded in the Data Breach Register of Hale Parish Council and reported to the ICO.

It was explained to members that the ICO's website affirms "Article 33(5) requires you to document the facts relating to the breach, its effects and the remedial action taken. This is part of your overall obligation to comply with the accountability principle, and allows us to verify your organisation's compliance with its notification duties under the GDPR."

"As with any security incident, you should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented - whether this is through better process, further training or other corrective steps."

It was confirmed that this breach had occurred due to action taken by a member of Hale Parish Council and further training was being arranged for all members at a further cost to the Council.

It was explained to members that the ICO's website affirms "When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it."

It was advised that in assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, or any other significant economic or social disadvantage to the natural person concerned.

It was explained to members that the ICO's website affirms "If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible."

"You will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In

such cases, you will need to promptly inform this affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach."

It was noted that Hale Parish Council must document its decision-making process in line with the requirements of the accountability principle.

Considerations In Favour of Disclosure	Considerations Against Disclosure
- Hale Parish Council must inform data subjects if there is a high risk to their rights / freedoms as a result of a breach of their personal information. The Council considered if the data breach could give rise to risks concerning the rights and freedoms of the data subjects. - The Council considered that the data is now in the public domain and could be shared further with public and press. - The data breach concerned two employees. One employee is aware of data breach which concerned their home address. Another employee is not yet aware of the data breach which contains allegations made against them. Hale Parish Council has a duty of care to employees to protect them from harm and should treat all employees consistently. The Council considered if one employee was aware of data breach, the other employee should also be made aware of data breach. - The Council considered the fact that the employee has already been made aware by the data breacher that a data breach may occur. - The Council considered non-disclosure may cause significant distress and anxiety to the employee if they experience impacts to their rights and freedoms, without being forewarned and/or forearmed. - If the Council refuse to disclose, the ICO have the power to compel an organisation to inform the affected individual, and the employee would then know anyway. The Council considered it could cause the employee significantly more adverse effects if they have to take this matter to the ICO and then find out the information at a later stage. - The Council considered the number of data breaches, and it cannot in good faith guarantee that this information won't be shared further, or be used against the data subject to harm their reputation and further rights and freedoms. - A member of the Council advised they were aware that there were actions being taken by a member of the Council that could affect the rights and freedoms of the employee - demonstrating risk of financial loss and damage to reputation. - A member of the Council noted how inappropriate it was for continuous breaches of data to be occurring so frequently and expressed dismay that the breaches appeared to originate from one member of the Council who was not acting appropriately.	- The disclosure could have an adverse effect on the employee.

The Council resolved to inform the data subject of the data breach.

5. The Council considered the release of recent complaint letters to the alleged perpetrator.

The Council were aware that the complainant was a member of the Council.

It was explained to members that page 36 of the ICO's Subject Access Code of Practice affirms "The Data Protection Act 1998 (DPA) says you do not have to comply with a SAR if to do so would mean disclosing information about another individual who can be identified from that information, except where it is reasonable in all the circumstances to comply with the request without that individual's consent.

"So, although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. If the other person consents to you disclosing the information about them, it would

be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

“You should make decisions about disclosing third-party information on a case-by-case basis. You must not apply a blanket policy of withholding it.

“For the avoidance of doubt, you cannot refuse to provide subject access to personal data about an individual simply because you obtained that data from a third party. The rules about third-party information, described in this chapter, apply only to personal data that includes information about the individual who is the subject of the request and information about someone else."

It was explained to members that page 37 of the ICO’s Subject Access Code of Practice affirms "As your obligation is to provide information rather than documents, you may delete names or edit documents if the third-party information does not form part of the requested information".

It was explained to members that page 38 of the ICO’s Subject Access Code of Practice affirms "in practice, it may sometimes be difficult to get third-party consent, eg the third party might refuse consent or might be difficult to find. If so, you must consider whether it is 'reasonable in all the circumstances' to disclose the information about the third party anyway.

"in some circumstances it will clearly be reasonable to disclose without trying to get consent, such as where the information concerned will be known to the requester anyway. Indeed it may not always be appropriate to try to get consent, for instance if to do so would inevitably involve a disclosure of personal data about the requester to the third party.

"confidentiality is one of the factors you must take into account when deciding whether to disclose information about a third party without their consent. A duty of confidence arises where information that is not generally available to the public (that is, genuinely 'confidential' information) has been disclosed to you with the expectation it will remain confidential. This expectation might result from the relationship between the parties.

“However, you should not always assume confidentiality. For example, a duty of confidence does not arise merely because a letter is marked 'confidential' (although this marking may indicate an expectation of confidence). It may be that the information in such a letter is widely available elsewhere (and so does not have the 'necessary quality of confidence'), or there may be other factors, such as the public interest, which mean that an obligation of confidence does not arise.”

It was explained to members that page 39 of the ICO’s Subject Access Code of Practice affirms “the following points are likely to be relevant to a decision about whether it is reasonable to disclose information about a third party in response to a SAR.

“- Information generally known to the individual making the request. If the third-party information has previously been provided to the individual making the request, is already known by them, or is generally available to the public, it will be more likely to be reasonable for you to disclose that information. It follows that third-party information relating to a member of staff (acting in the course of their duties), who is well known to the individual making the request through their previous dealings, would be more likely to be disclosed than information relating to an otherwise anonymous private individual.

“- Circumstances relating to the individual making the request. The importance of the information to the requester is also a relevant factor. The need to preserve confidentiality for a third party must be weighed against the requester's right to access information about his or her life. Therefore, depending on the significance of the information to the requester, it may be appropriate to disclose it even where the third party has withheld consent.”

It was explained to members that page 40 of the ICO’s Subject Access Code of Practice affirms "If you have not got the consent of the third party and you are not satisfied that it would be reasonable in all circumstances to disclose the third-party information, then you should withhold it. However, you are still obliged to communicate as much of the information requested as you can without disclosing the third-party individual's identity. Depending on the circumstances, it

may be possible to provide some information, having edited or 'redacted' it to remove information that would identify the third-party individual.

"You must be able to justify your decision to disclose or withhold information about a third party, so it is good practice to keep a record of what you decide, and why."

It was noted that Hale Parish Council must document its decision-making process in line with the requirements of the accountability principle.

Considerations In Favour of Disclosure	Considerations Against Disclosure
- The Council considered that the data subject has rights to their own personal data. - The Council considered it cannot refuse to provide subject access to personal data about an individual simply because it obtained that data from a third party. - The Council considered if the letter had the necessary quality of confidence after being shared with third parties. - The Council considered that the third-party information had previously been provided to the data subject making the request. - The Council considered that the complainant had revealed their identity to the data subject and made the data subject aware that a letter of complaint had been written about them. - The Council considered that the third-party information had been made available to members of the public and additional third parties. - The Council considered the information is now in the public domain and could be shared further with public and press. - The Council considered the importance of the information to the requester. - The Council considered whether it would be reasonable in all the circumstances to disclose the third party information about the complainant. - Hale Parish Council considered its duty of care to its employees. - The Council considered non-disclosure may cause significant distress and anxiety to the data subject. - If the Council refuse to disclose, the ICO have the power to compel an organisation to release the information, and the data subject would then know anyway. The Council considered it could cause the employee significantly more adverse effects if they have to take this matter to the ICO and then find out the information at a later stage. - The Council considered the number of occasions where confidential information has been shared by the complainant, and it cannot in good faith guarantee that this information won't be shared further, or be used against the data subject. - The Council noted an email sent by the complainant on the day of the alleged offence (3 December 2019) advising that it was "nice to see" the data subject and "we had a very interesting chat". These statements were inconsistent with allegations written in the first complaint letter dated 19 December 2019. The Council considered whether non-disclosure would set a precedent for letters containing inconsistent allegations that could then be used to damage the reputation of a data subject through the disclosure of the allegations to third parties. - The Council considered if it had failed by not having any clear policies in place that would restrict the data subject from visiting the residence of a Councillor.	- The Council considered that the third party had refused to give their consent. - The Council considered that the third party has rights.

The Council resolved to release the recent complaint letters.

Cllr Cleary exited the meeting.

6. **The Council resolved to explore additional HR Service providers at a more economical cost than the quote considered.**