

WEST LANCASHIRE BOROUGH COUNCIL – WHISTLEBLOWING CODE

CONSULTATION RESPONSES

CONSULTATION RESPONSE	RECOMMENDATION	ADOPTED?
<p>RESPONSE 1 WLBC – DATA PROTECTION OFFICER</p>	<p>Having read the current and proposed "Whistleblowing Code", I thought it maybe useful to provide you with this feedback for consideration prior to its rollout.</p> <p>The Public Interest Disclosure Act 1998 (PIDA 1998), which is also now incorporated into the Employment Rights Act 1996 (part IVA). You may wish to mention the Employment Rights Act 1996 legislation as well within the proposed Whistleblowing Code.</p> <p>With the introduction of UK GDPR, it has made privacy rights even more stringent, increasing the need to carry out the proposed whistleblowing procedure with careful internal checks and controls as I will elaborate as follows;</p> <p><u>The Right to be Forgotten</u></p> <p>UK GDPR also underlines the ‘Right to be Forgotten’. This includes the requirement that personal data be erased after being completely processed. GDPR (Article 17) describes "the conditions for the erasure of data": either the data is no longer relevant to the original purposes of processing, or the data subject withdraws his or her consent for data processing. In contrast to email or phone reporting, WLBC's whistleblowing will need to meet these erasure requirements by providing where relevant options like data anonymization in a simple and structured manner.</p> <p>The UK GDPR gives individuals significant rights regarding their personal data. Some of these rights may potentially conflict with the public interest in protecting whistleblowers against the risk of retaliation for making a protected disclosure.</p> <p>For example, if say employee A discloses information about employee B to an employer and employee B later makes a subject access request under DPA, employee B has a right of access to their personal data, including “where personal data are not collected from the data subject, any information as to their source” which would in reality reveal the identity of the whistleblower.</p> <p>If access is granted to a concerned individual, all the personal data of the whistleblower and any third parties should therefore be redacted from those documents. This is where the "Whistleblowing SOP" will come into play. Where this is not practicable, it may be possible to withhold the disclosure of an individual’s personal data on the basis that this would interfere with the rights and freedoms of another individual. This will need to be assessed on a case-by-case basis in practice by the Data Protection Officer in consultation with the Monitoring Officer and Internal Audit Manager.</p> <p>To comply with data protection obligations, WLBC must</p>	<p>Adopted</p> <p>The guidance provided by the DPO is very useful and although it will not form part of the Code itself the requirements of GDPR will be included in the working practices that will be developed once the Code is adopted to ensure compliance with the regulations</p>

ensure we adhere to strict internal procedures when handling whistleblowing cases as part of this code and SOP. This should include the following steps which is to be considered as a minimum:

- **limit the processing of personal data to that which is necessary.**

A whistleblower may pass on information that is irrelevant to the allegations, in which case it is the Monitoring Officer and the Internal Audit Managers responsibility to restrict and delete any extraneous information, particularly that relating to special categories of data, to ensure that the information that is passed on is limited to that which is strictly needed for the investigation in consultation with the Data Protection Officer and Information Governance team.

- **limit the amount of time for which the personal data is held under WLBC's Records Retention Policy.**

Once the investigation has concluded, extract the personal data held from day-to-day systems and implement technical and organisational measures to hold the personal data securely in line with the councils Data Protection and Security Policies.

- **inform relevant categories of individuals that their personal data is being processed (where possible).**

For example, the whistleblower should be told, in general terms, who the possible recipients of their disclosures and personal data could be as part of the proposed whistleblowing code. Informing third parties (such as regulators) may not be necessary where this would be disproportionate, so this can be assessed on a case-by-case basis.

I also feel a section on Data Protection needs to be included and embedded possibly in beginning of the Whistleblowing Code as follows taking into consideration some of my initial observations as highlighted to you above;

Data protection

- a) A disclosure made under this policy is likely to identify an individual or individuals, or may lead to an investigation in which it is necessary to identify individuals. It will therefore involve the processing of personal data under the Data Protection Act 2018 (DPA) and General Data Protection Regulation 2016 (GDPR). Depending on the nature of the allegations or information disclosed it may also involve the processing of special category personal data and/or personal data relating to criminal offences and convictions.
- b) WLBC's lawful basis for processing personal data in response to a disclosure made under this policy including special category data is set out in our

	<p>corporate Privacy Notice.</p> <p>c) Individuals named in a disclosure will normally be told of the allegations and the identity of anyone who will receive personal data about them during the investigation of the matter, unless there is a substantial risk that this will prejudice the investigation or it would otherwise be unlawful.</p> <p>d) All personal data collected during receipt and investigation of a concern raised under this policy will be processed fairly and lawfully in accordance with UK GDPR and the Data Protection Act 2018. From the information gathered, the retention and processing of personal data will be restricted to what is necessary for the purpose of investigating and responding to the concern raised. Personal data may need to be shared with relevant third parties in the course of investigating or responding to a concern raised; this will only happen where it is fair, lawful and necessary (to the extent such steps are required by applicable data protection laws) for the proper investigation and resolution of the matter. Where it is necessary to share information with third parties, this will be restricted to information which is needed for the investigation and WLBC will redact or anonymise personal data where it is possible to do so without compromising the purpose of the investigation.</p> <p>e) Personal data gathered will be kept until the end of the investigation or any subsequent legal, regulatory or disciplinary proceedings and any necessary data will be retained securely for seven years after the close of the case or in accordance with WLBC's Records Retention Schedule. After the retention period has lapsed any personal data will be securely destroyed in accordance with the councils Records Management Policy.</p> <p>f) The Monitoring Officer and Internal Audit Manager will ensure that a data protection impact assessment (DPIA) is carried out before the processing of personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals.</p> <p>I trust this feedback is useful...</p>	
<p>RESPONSE 2</p> <p>AUGHTON PARISH COUNCIL</p>	<p>Revised Whistleblowing Code - members noted the policy aims, scope and purpose and the Whistleblowing Flowchart was most helpful. We have no comments to raise on the revised Code.</p>	<p>No action required</p>

<p>RESPONSE 3 Member of Staff</p>	<p>My feedback relates to the flow, if I follow the route of No – I don't believe a wrongdoing has happened, is happening or is likely to happen, what are the reasons I would be referring to my line manager? Is it because:</p> <ol style="list-style-type: none"> 1. I am not sure if my concerns are a case of whistle blowing or 2. I have a concern that would be managed via a different route? <p>I think it is the latter as 3.4 quotes: If you are uncertain whether your concern amounts to a whistleblowing concern, you should seek advice from the Monitoring Officer on the details below or alternatively, you may seek advice externally from Protect the independent whistleblowing charity, who offer a confidential helpline. Protect's contact details can be found at Annex 1.</p> <p>If I was being lazy and not reading the policy and solely looking at the flow, I am not sure I would know what to do, if I was not sure if it was a whistle blowing issue.</p>	<p>Amendments have been made to the Whistleblowing Flowchart to clarify the situation.</p> <p>In the example given if the activity doesn't fall under this code it doesn't mean that it is not something that should still be looked at hence the request to refer the issue to their line manager to consider other appropriate lines of enquiry.</p> <p>If they are unsure as to whether the issue falls under the Code they can consult the Monitoring Officer or Protect the independent whistleblowing charity.</p>
---------------------------------------	---	--