TRANSFORMATION AND IMPROVEMENT OVERVIEW AND SCRUTINY COMMITTEE

9 FEBRUARY 2026

RESPONSE TO PUBLIC QUESTIONS

1. John Palmer

Question:

Near the end of the Performance Monitoring Report Q3 2025/26, in the Table listing all the Exceptions, it is revealed that no less than 6 personal data breaches in Q3 were of the most serious Level 3, and thus had to be reported to the Information Commissioner's Office. These were part of 52 personal data breaches in the 3-month period overall.

Will the Chair be raising this concerning data for committee to discuss in today's meeting?

It is curious that the report states a decision was made in September 2025 at an IGLOO meeting to overhaul a failing internal cascade reporting system, but admits that over 4 months on, no report template to do so has been made. Does this shine a light on whether the council is taking personal data security as seriously as it should?

Response:

Thank you for your question Mr Palmer.

I am sure members will wish to discuss this item now that attention has been drawn to it.

In terms of your wider question, the Council takes its responsibility for information security extremely seriously. When a personal data breach occurs, the council's Information Governance team (IGT) assesses the likelihood of the risk to people's rights and freedoms. Legislation states that '**if a risk is likely'**, the ICO must be notified. There is no formal framework for assessing the risk and it can depend on the personal circumstances of the person affected.

In all cases where the council has heard back from the ICO, the council has been found to have taken all necessary actions in response to the breach. The ICO offers advice as a matter of course, but this is already included in our current procedures.

The council takes the following steps to prevent breaches occurring:

- All staff are required to undertake annual data protection and cyber awareness training and in all cases reported, the training has been completed and staff understand their role in protecting information.

- There is a procedure in place for reporting breaches. The new training introduced in December 2025 includes details of how to do this. Guidance is included on the Council's Intranet.
- At the time an incident is reported, IGT look into the cause and identify any actions that should be taken to reduce the likelihood of a similar breach happening again.

The quarterly cascade from IGLOO was one additional step that we identified could be implemented. This would be to support Managers so they can monitor the number and cause of breaches and identify any improvements that could be made. Instead, IGT is taking steps to report more frequently to Service Directors, and in 2026 a monthly report will be provided. The first report being provided by mid-February 2026 when details from January will be available."