

## **Supplement to the agenda**

### **Audit and Governance Committee**

Tuesday 29 September 2026, 2.00 pm

Herefordshire Council Offices, Plough Lane, Hereford, HR4 0LE

#### **Contents**

| <b>Item</b> | <b>Title and purpose</b>                                                                                | <b>Page(s)</b> |
|-------------|---------------------------------------------------------------------------------------------------------|----------------|
| <b>5.</b>   | <b>Questions from members of the public</b><br><br>To receive any questions from members of the public. | <b>3 - 4</b>   |





## PUBLIC QUESTIONS TO AUDIT AND GOVERNANCE – TUESDAY 29 SEPTEMBER 2026

### Question 1

Ms Reid, Hereford

To: Chair of Audit and Governance

“An article on the website of UKAuthority Office was entitled ‘Herefordshire council employee pleads guilty to data misuse’. The article included: “Over a four-day period, [presumed former employee] unlawfully accessed approximately 490 records and downloaded 94 documents, including highly sensitive material such as medical records, social worker reports, and child and family assessments. ... Andy Curry, ICO head of investigations, said: ‘Smith abused his position as an employee and used his access to Herefordshire Council’s systems to view the personal information of people known to him, without any legitimate reason to do so. The sensitive nature of the records held within a Children and Young People directorate, and Smith’s systematic misuse of that information, makes this particularly serious.’” Can other employees access without a legitimate reason?”

### **Response**

*“Thank you for drawing the attention of the Committee to this matter.*

*Employees are not authorised to access personal information unless they have a legitimate reason to do so as part of their role. As highlighted by the Information Commissioner’s Office in this case, the employee abused their position by accessing personal information without a legitimate reason.*

*As part of their role, the employee was trained and given access to the Mosaic case management system. Training must be completed before access is granted, and employees are informed that they must only access records where there is a business purpose for doing so. Employees are also required to notify their manager if they are aware, or become aware, that they know someone whose records are held on the system, so that access to those records can be blocked.*

*Following this incident, all staff and managers have been reminded that access to Council systems and information is for business purposes only. A new system for auditing access is being rolled out, the arrangements for officers notifying managers of people they know have been improved, and these requirements are reinforced through mandatory training for new staff and annually thereafter.*

*The Council takes the protection of personal information seriously and will take appropriate action where an employee misuses their access to sensitive information”.*

