West Yorkshire Combined Authority | Tracy Brabin Mayor of West Yorkshire

Our Reference: 2719

26/02/2026

Freedom of Information Act 2000 Enquiry: Cyber or information security

Thank you for contacting West Yorkshire Combined Authority ('the Combined Authority') with your request for information, which was received on 09/01/2026. Your request was:

"Please provide the following information for the period 1 Jan 2023 – 31 Dec 2024:

1. The number of occasions on which cyber or information security risks appeared on the agenda of your governing body (or equivalent oversight body).

2. The name(s) of any committee(s) or board(s) with formal responsibility for cyber or information security oversight.

3. Whether documented criteria exist for escalating significant cyber incidents to the governing body or senior leadership (yes/no; if yes, please provide or summarise).

4. The number of governing body members (or equivalent) who completed cyber or information security training during this period, and the total number of members in that body.

5. Whether an independent assessment of your cyber security arrangements (e.g. internal audit, external review, or third-party assessment) was reported to the governing body during this period (yes/no; if yes, please state the type of assessment).

Please note: no technical details, vulnerabilities, or sensitive operational information are requested. If this information is readily available, broken down by year, please provide it; otherwise, an aggregate figure for the period is sufficient."

This request was handled under the Freedom of Information Act 2000 (FoIA) and I can confirm that the Combined Authority holds the information covered by your request.

We have now concluded our assessment regarding whether the information requested was exempt under Section 31(1)(a) of the Freedom of Information Act 2000 where disclosure would or would be likely to prejudice the prevention or detection of crime.

In line with the terms of this exemption in the FoIA, the organisation has considered whether it would be in the public interest for us to provide you with the information, so we have looked at whether the disclosure covered information that could be exploited for criminal gain, and the likelihood of that happening.

The risk of releasing information into the public domain was considered minimal, and unlikely to cause prejudice against law enforcement purposes. We therefore consider that, for this reason, the public interest in disclosing the information outweighs that of the public interest in withholding it from disclosure, please find our full response below:

For the period 1 January 2023 – 31 December 2024:
1. The number of occasions on which cyber or information security risks appeared on the agenda of your governing body (or equivalent oversight body).

Cyber or information security risks go to the Corporate Scrutiny Committee and the Audit and Governance Committee as part of the Combined Authority's risk register. There was 1 occasion during the period requested that the agenda included this topic; please see below and the files attached:

Corporate Scrutiny Committee - 01 Mar 24

Ref 2719 - 20240301 Agenda doc public pack - Corporate Scrutiny Committee.pdf
Ref 2719 - 20240301 Agenda frontsheet - Corporate Scrutiny Committee.pdf
Ref 2719 - 20240301 Item 8 Cyber Security - Corporate Scrutiny Committee.pdf

These relate to the Corporate Scrutiny Committee meeting of 1st March 2024, the details of which are published on our website. This link takes you to a search function where you can search for agendas, reports and minutes from previous committee meetings: WYCA - Modern Gov

The following links to meetings are included as they may contain related information where the topic of cyber security was mentioned although was not an agenda item:

- Corporate Scrutiny Committee - 20 Jan 23
- Business Economy & Innovation Committee - 24 Jan 23
- Finance Resources & Corporate Committee - 07 Mar 24

2. The name(s) of any committee(s) or board(s) with formal responsibility for cyber or information security oversight.

- Regulatory & Compliance Board – a previous board which had an oversight role during the timeframe of the request, rather than a governing one
- Governance & Audit Committee
- Corporate Scrutiny Committee
- Finance, Resources, & Scrutiny Committee

3. Whether documented criteria exist for escalating significant cyber incidents to the governing body or senior leadership (yes/no; if yes, please provide or summarise).

Yes. We have a Cyber Incident Response Plan (CIRP), a Major Incident Plan, and an Incident Management & Business Recovery Plan (IMBR). Based on the security of the incident being dealt with, certain escalation routes are defined, from activation of a Cyber Incident Response team to activation of Gold Command.

There is also a Data & Cyber Security Incident Procedure that all staff must familiarise themselves with, containing sections that cover escalations to senior leaders/boards for 'significant' incidents, which read as follows:

"The DPO will notify the SIRO all incidents that are categorised as high risk, or in the opinion of the DPO should involve the SIRO. The SIRO's responsibilities are outlined under 'Roles and responsibilities'.
…
Incidents with a higher risk level may necessitate a Summary Report, setting out the key details of the incident; any recommendation or required further action; details of notifications to third parties and any feedback from the ICO (where given). This will be sent for information to the relevant IAO and the SIRO, and potentially to other key members of staff, Gold Steering Group, or Regulatory and Compliance Board."

4. The number of governing body members (or equivalent) who completed cyber or information security training during this period, and the total number of members in that body.

No governing body members completed cyber or information security training during the period requested. However, the Regulatory & Compliance Board was composed of Combined Authority staff who would have completed cyber security training during 2023-24, and cyber security training was introduced as mandatory for all Combined Authority staff from September 2024.

5. Whether an independent assessment of your cyber security arrangements (e.g. internal audit, external review, or third-party assessment) was reported to the governing body during this period (yes/no; if yes, please state the type of assessment).

Yes. External penetration tests were undertaken during that period.

If you believe that your request for information has not been handled properly, you can ask for an internal review of our decision. Internal review requests should be submitted within two months of the date of receipt of this letter.

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 0303 123 1113
Website: www.ico.gov.uk

For your information, there is no charge for making an appeal.

Yours sincerely,
Information Governance Officer
freedom.info@westyorks-ca.gov.uk