From: EIR Compliance

To:

Subject: 20251110 - EIR - Response

Date: 10 November 2025 10:05:00

Reference Number: **EIR**

Dear

We refer to your request for environmental information submitted to Yorkshire Water dated 15 October 2025:

"I am writing to make a request for information under the Environmental Information Regulations 2004 (EIR), seeking information held by your company relating to cyber incidents that have had, or could have had, an environmental impact on your operations or services.

Specifically, please provide:

1. *The number of qualifying cyber incidents experienced by your company in each of the last four calendar years (i.e. 2021-2025), where the incident*:
    - *had a direct or potential effect on water treatment, wastewater management, discharge, water quality, or environmental monitoring systems, or*
    - *otherwise affected your ability to prevent or mitigate harm to the environment.*
1. *For each year, please indicate in summary form the known or potential environmental consequences of those incidents (for example, whether any discharge limits were exceeded, whether environmental monitoring or reporting was affected, or whether any pollution or supply incidents were recorded as a result).*

I am not seeking any operational or security-sensitive detail, such as the systems affected, the technical vulnerabilities exploited, or information about your security posture, suppliers, or defences.

The information sought is limited to the numerical count per year of incidents, and a description of the environmental outcomes, which are squarely within the definition of environmental information under Regulation 2(1)(f) of the EIR —

being "measures (including administrative measures)… affecting or likely to affect the elements and factors of the environment."

Cyber incidents that disrupt water or wastewater operations, or your ability to monitor or report on them, are measures or events affecting the state of water and related environmental factors, and therefore fall within that definition.

Disclosure of this information would be in the public interest because:

- *It enables the public to understand the resilience of environmental infrastructure (specifically, water and wastewater systems) to cyber events that could directly affect the environment.*
- *It promotes accountability and environmental protection, by showing whether cyber risks have had observable environmental effects.*
- *The request is narrow in scope — seeking only aggregated annual counts and environmental impact information — so it does not prejudice national security, public safety, or commercial confidentiality.*
- *Providing this limited information helps fulfil the public's right under the EIR to know how environmental risks are managed, while avoiding disclosure of any sensitive technical or security information.*

On this basis, the public interest in disclosure clearly outweighs any potential interest in withholding the limited, aggregated information requested.

Please provide the information requested in any convenient format (e.g. a simple table or summary document).

If any part of the request is considered too broad or unclear, please let me know so that I can refine it.

If you believe any exemptions (exceptions) apply, please provide the specific Regulation relied upon and the reasoning, including how the public interest test has been applied."

In accordance with section 12(5) paragraph (a) of the EIR, a public authority may refuse to disclose information to the extent that its disclosure would adversely affect international relations, defence, national security or public safety. Whilst we understand that for the purposes of public interest it would be beneficial to obtain this information we also have to considered whether it would be in the wider public interest to disclose the information. When weighed against the potential risk to national security and public safety we are refusing to confirm or deny

whether we hold information relating to cyber incidents affecting critical national infrastructure.

Revealing whether such information is held could in itself pose a risk to national security. Confirmation or denial may provide malicious actors with intelligence regarding the presence or absence of cyber events resulting in targeting our critical infrastructure. This would undermine protective measures and could facilitate attacks, which would compromising the safety and resilience of essential services.

Safeguarding national security includes the protection of potential targets, even if there is no evidence that an attack is imminent. The clean water, wastewater networks and our IT systems form part of the Critical National Infrastructure (CNI) of this country and could be perceived as a potential target for such an attack.

As part of our legal and regulatory responsibilities in line with Security and Emergency Measures Direction, a statutory instrument under the Water Industry Act 1991, we must ensure that information which could be used to threaten national security is protected.

While there is a general public interest in transparency and accountability in line with the Environmental Information Regulations (EIR), in this case we consider the overriding interest is in safeguarding national security and public safety to ensure the continued operation of critical services. Disclosure even at the level of numeric confirmation or denial of cyber incident could have detrimental consequences.

We trust that the provision of this data satisfies your request. In accordance with the Environmental Information Regulations 2004, if you are not satisfied with this reply to your request you can ask for an internal review. A request for an internal review must be submitted within 40 working days by contacting the Data Protection Team.

Thank you for contacting Yorkshire Water.

Yours sincerely,

Data Protection Team

Email: EIR@Yorkshirewater.co.uk