Ref. No:	1263
Date:	10/10/24
Subject:	Auto forward rules

REQUEST

We are currently looking into our auto forward rules within our Trust as this creates a lot of issues for our IT department. I would be very grateful if you could advise how you handle this within your Trust, please can you provide answers to the following questions:

1. **Does your Trust allow staff to auto forward from their work email address, either to personal or additional work email addresses?**

2. **Does your Trust allow staff to add rule based forwards from their work email address?**

3. **If auto forward is allowed, do you have a policy or guidance of when this is allowed?**

4. **How do Monitor auto forward when in place?**

RESPONSE

Section 31(1)(a) will cover all aspects of the prevention and detection of crime…The exemption also covers information held by public authorities without any specific law enforcement responsibilities…It could also be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures.

Information disclosed under Freedom of Information becomes publicly available. This means that the impact of disclosure must be considered from the general release of information and not limited to disclosure to one individual (the requestor).

The Trust determines that to disclose the requested information could be used by cyber criminals to identify our preparedness for a cyber-attack. The Trust is therefore exempting this response.

As part of phishing attacks and account compromise putting auto forwards on emails is one method threat actors will use to exfiltrate data out of the

organisation. As such providing what controls we may or may not have around this area could provide malicious actors information on how to get around these controls.