



Ministry of Justice

N Gilliatt

fFaudwAtch UK <request-339790-ec47c9e2@whatdotheyknow.com>

Christine Lewis
Interim KILO
MoJ Digital and Technology
11.51, 102 Petty France
London SW1H 9AJ

data.access@justice.gsi.gov.uk
www.gov.uk

Our Reference: 105896

21 June 2016

Freedom of Information Request

Dear N Gilliatt,

Thank you for your email of 13 June, in which you asked for the following information from the Ministry of Justice (MoJ):

Below is contained in correspondence dated 2 March 2016 from Grimsby Magistrates' court in relation to an information served by email attachment.

" I note that you have attached a document to your e-mail. I have been advised by a member of the IT department not to open the attachment, due to the fact that an attachment in a previous email contained a virus. "

I would like disclosing all instances of computer virus issues recorded by the IT department at Grimsby Magistrates' court between December 2015 and March 2016 with a brief description of each threat.

Your request has been handled under the Freedom of Information Act 2000 (FOIA).

I can confirm that the department holds information that you have asked for, but in this case we will not be providing it to you as it is exempt from disclosure.

We are not obliged to provide information if its release would prejudice law enforcement. In this case, we believe that releasing the information would be likely to prejudice the prevention or detection of crime (section 31(1) (a) of the Act).

In line with the terms of this exemption in the Freedom of Information Act, we have also considered whether it would be in the public interest for us to provide you with the information, despite the exemption being applicable. In this case, we have concluded that the public interest favours withholding the information.

You can find out more about Section 31 by reading the extract from the Act and some guidance points we consider when applying this exemption, attached at the end of this letter.

You can also find more information by reading the full text of the Act, <http://www.legislation.gov.uk/ukpga/2000/36/section/31> and further guidance

When assessing whether or not it was in the public interest to disclose the information to you, we took into account the following factors:

Public interest considerations favouring disclosure

- Disclosure of the information would be consistent with policies for greater transparency about the uses of, and accountability for, public expenditure.
- It is also in the public interest to know that a public authority has measures in place to protect information in their possession and to mitigate the impact of a malware attack.

Public interest considerations favouring withholding the information

- Disclosure of any information about the security systems on computer systems would make them more vulnerable to interference by potentially assisting criminal activity.
- We believe that details of whether the IT department at Grimsby Magistrates' Court has suffered from any computer virus issues would provide information which could be used maliciously against our systems. It could also prejudice both the prevention and detection of a crime, and/or the apprehension of offenders.
- Attempts to breach the security of Government IT systems could lead to a loss of confidentiality, integrity and potential availability of information on an ICT system. Consequences of potential security breaches may include some or all of the following:
 - ☐ malfunction of software
 - ☐ breaches of physical security arrangements;
 - ☐ theft or loss of software;
 - ☐ misuse of software;
 - ☐ use of unauthorised or unlicensed software;
 - ☐ uncontrolled system changes;
 - ☐ theft or loss of data;
 - ☐ malicious software (e.g. computer virus);
 - ☐ wilful damage to information;
 - ☐ loss of service;
 - ☐ system malfunctions or overloads;
 - ☐ unauthorised use of a computer;
 - ☐ unauthorised amendment of information or software held on a computer;
 - ☐ unauthorised disclosure of information;
 - ☐ non-compliance with policies or guidelines;

We reached the view that, on balance, the public interest is better served by withholding this information under section 31(1) (a) of the Act at this time.

You have the right to appeal our decision if you think it is incorrect. Details can be found in the 'How to Appeal' section attached at the end of this letter.

Disclosure Log

You can also view information that the MoJ has disclosed in response to previous FOI requests. Responses are anonymised and published on our on-line disclosure log which can be found on the MoJ website:
<https://www.gov.uk/government/organisations/ministry-of-justice/series/freedom-of-information-disclosure-log>

Yours sincerely

Christine Lewis

How to Appeal

Internal Review

If you are not satisfied with this response, you have the right to an internal review. The handling of your request will be looked at by someone who was not responsible for the original case, and they will make a decision as to whether we answered your request correctly.

If you would like to request a review, please write or send an email **within two months of the date of this letter** to the Data Access and Compliance Unit at the following address:

Data Access and Compliance Unit (10.34),
Information & Communications Directorate,
Ministry of Justice,
102 Petty France,
London
SW1H 9AJ

E-mail: data.access@justice.gsi.gov.uk

Information Commissioner's Office

If you remain dissatisfied after an internal review decision, you have the right to apply to the Information Commissioner's Office. The Commissioner is an independent regulator who has the power to direct us to respond to your request differently, if he considers that we have handled it incorrectly.

You can contact the Information Commissioner's Office at the following address:

Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire
SK9 5AF

Internet address: https://www.ico.gov.uk/Global/contact_us.aspx

EXPLANATION OF FOIA – SECTION 31 - LAW ENFORCEMENT

We have provided below additional information about Section 31 of the Freedom of Information Act. We have included some extracts from the legislation, as well as some of the guidance we use when applying it. We hope you find this information useful.

The legislation

Section 1: Right of Access to information held by public authorities

- (1) Any person making a request for information to a public authority is entitled—
- (a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and
 - (b) if that is the case, to have that information communicated to him.

Section 31: Law Enforcement

(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—

- (a) the prevention or detection of crime,
- (b) the apprehension or prosecution of offenders,
- (c) the administration of justice,
- (d) the assessment or collection of any tax or duty or of any imposition of a similar nature,
- (e) the operation of the immigration controls,
- (f) the maintenance of security and good order in prisons or in other institutions where persons are lawfully detained,
- (g) the exercise by any public authority of its functions for any of the purposes specified in subsection (2),
- (h) any civil proceedings which are brought by or on behalf of a public authority and arise out of an investigation conducted, for any of the purposes specified in subsection (2), by or on behalf of the authority by virtue of Her Majesty's prerogative or by virtue of powers conferred by or under an enactment, or
- (i) any inquiry held under the Fatal Accidents and Sudden Deaths Inquiries (Scotland) Act 1976 to the extent that the inquiry arises out of an investigation conducted, for any of the purposes specified in subsection (2), by or on behalf of the authority by virtue of Her Majesty's prerogative or by virtue of powers conferred by or under an enactment.

(2) The purposes referred to in subsection (1)(g) to (i) are—

- (a) the purpose of ascertaining whether any person has failed to comply with the law,
- (b) the purpose of ascertaining whether any person is responsible for any conduct which is improper,
- (c) the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise,

- (d) the purpose of ascertaining a person's fitness or competence in relation to the management of bodies corporate or in relation to any profession or other activity which he is, or seeks to become, authorised to carry on,
- (e) the purpose of ascertaining the cause of an accident,
- (f) the purpose of protecting charities against misconduct or mismanagement (whether by trustees or other persons) in their administration,
- (g) the purpose of protecting the property of charities from loss or misapplication,
- (h) the purpose of recovering the property of charities,
- (i) the purpose of securing the health, safety and welfare of persons at work, and
- (j) the purpose of protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work.

(3) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

Guidance

Section 31 is concerned with protecting a wide range of law enforcement interests and its application turns on whether disclosure would be likely to prejudice those interests.

Some interests that are protected by section 31 are drawn quite widely, for example: the administration of justice, the prevention or detection of crime and the operation of immigration controls. But section 31 also applies where the exercise by any public authority of certain specified functions would be prejudiced by disclosure. Those functions include: ascertaining whether a person is responsible for improper conduct, determining the cause of an accident and ascertaining a person's fitness to carry on a profession.

This section is not restricted to information of any particular description; it turns on consideration of the likely effects of any disclosure. Examples of circumstances in which the prejudicial effects referred to in this part of this exemption are most likely to be relevant could include the following disclosures:

- intelligence about anticipated criminal activities
- information relating to planned police operations, including specific planned operations, and policies and procedures relating to operational activity;
- information relating to the identity and role of police informers
- information relating to police strategies and tactics in seeking to prevent crime
- information whose disclosure would facilitate the commission of any offence; and
- information whose disclosure would prejudice the fair trial of any person against whom proceedings have been or may be instituted.