National Police
Freedom of Information
and Data Protection Unit

NPCC
National Police Chiefs' Council

c/o PO BOX 481
Fareham
Hampshire
PO14 9FS

Tel: 02380 478922
Email: npcc.foi.request@npfdu.police.uk

12/07/2023

FREEDOM OF INFORMATION REQUEST REFERENCE NUMBER: 167/2023

Thank you for your request for information regarding NPCC CyberAlarm, which has now been considered.

Applicant Question:

Dear National Police Chiefs' Council,

As part of reviewing school support, I am looking to determine the feasibility of using CyberAlarm, instead of just registering like most do.

Completing supplier chain risk assessments to support school Data Protection Officers is sometimes a thankless task, but I am hoping you can help with some information.

1. Please provide a public copy of any data processing agreement or data sharing agreement that exists between any parties involved, i.e. the school, NPCC, the provider, any related contractors.

2. Please provide copies of relevant risk assessments completed by NPCC, as set out in guidance by the ICO on DPIAs and other risk assessments.

3. Please provide details of organisations selected by NPCC or the provider to complete any risk assessments, along with copies of these reports.

I fully understand the requirement to protect some of the above information, and will happily accept any redactions that are made.

Please be aware that without sufficient information schools CANNOT complete their own risk assessments and so CANNOT make use of the CyberAlarm systems.

NPCC Response:

The NPCC does hold information captured by your request.

Some of the captured documents have been subject to redactions and two documents have been withheld in full by virtue of the following exemptions:

Section 21 Reasonably accessible by other means, Section 23(1) Information relating to Security Bodies, Section 31(1) Law enforcement, Section 40(2) Personal Information, Section 41(1) Information Provided in Confidence, S42(1) Legal Professional Privilege and Section 43(2) Commercial Interests.

For ease of understanding, I have provided a full list of captured information and the relevant engaged exemptions below. Further information relating to the above exemptions can be found at Annex A below.

Some of the documents contained embedded documents. Whilst forming part of the documents, and therefore captured by the FOI legislation, I have extracted the embedded documents and provided by way of separate attachments for ease of reading and formatting. For information, two of the embedded DPIAs (2021.04.26 PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded docs 1 & 2)) are now out of date. I have annotated each extraction with the reference to the attachments for convenience:

In wishing to assist you, the ICO Guidance on the use of cloud computing that has been withheld citing Section S21 Reasonably accessible by other means is available at the following link: Guidance on the use of cloud computing (ico.org.uk)

Outside of the Freedom of Information Act, my colleagues provided the following information by way of explanation to try and assist you:

Police CyberAlarm is one of a number of initiatives established and co-ordinated by the National Police Chiefs' Council's National Cybercrime Programme, hosted by the City of London Police, on behalf of police forces throughout the United Kingdom in support of the National Cyber Security Strategy to make Britain secure and resilient in cyberspace, in particular to defend against and deter cybercrime.

At the outset we wish to make clear that, as set out in the Member Organisation Agreement entered into between forces and Police CyberAlarm member organisations, police forces do not act as a data processor on behalf of member organisations in connection with the provision of data, including any personal data, by member organisations to police forces. In such circumstances, we do not consider that it is necessary for member organisations, or potential member organisations, to have access to all of the requested documentation in order to fulfil their own legal and regulatory obligations pertaining to the sharing of data, which may include personal data, with police forces for law enforcement purposes under the auspices of Police CyberAlarm.

In relation to question 1, we can confirm that data processing agreements are in place between police forces and the supplier, and that a copy of these agreements is held for the purposes of FOIA. We enclose a copy of the data processing agreement between police forces and the supplier. We can confirm that a data sharing agreement is in place between member organisations and police forces, and that a copy of this agreement is held for the purposes of FOIA. We enclose a copy of the Member Organisation Agreement.

In relation to question 2, we can confirm that a Data Protection Impact Assessment was conducted prior to the deployment of the current iteration of Police CyberAlarm (as was the case in relation to the previous iteration of the system) and that a copy of this is held for the purposes of FOIA. We should clarify that while a Data Protection Impact Assessment has been carried out, that does not necessarily indicate that an Assessment was considered to be mandatory in accordance with the requirements of data protection law. We enclose a copy of the current Data Protection Impact Assessment.

We can also confirm that a Community Impact Assessment and an Equality Impact Assessment were conducted in relation to Police CyberAlarm, and that copies of these are held for the

purposes of FOIA. We enclose a copy of the current Community Impact and Equality Impact Assessment.

In relation to question 3, we can confirm that an Information Risk Assessment was conducted by the Police Digital Service prior to the deployment of the current iteration of Police CyberAlarm as part of the wider cyber security measures. We enclose a copy of the Information Risk Assessment and related documents.

	Document	**Exemptions**
Question 1	2021.12.01 PCA 2.0 Member Agreement Final	Released in full.
	2021.12.01 Service Recipient-Supplier Agreement	S31(1) Law Enforcement, S40(2) Personal Information, S43(2) Commercial Interests
	2021.12.03 Inter-force agreement	S23(1) Security Bodies
	2021.12.09 Signed Agreement with Supplier	S31(1) Law Enforcement S40(2) Personal Information, S41(1) Information Provided in Confidence S43(2) Commercial Interests
Question 2		
	2021.12.03 PCA DPIA Stage 1	S23(1) Security Bodies S40(2) Personal Information S31(1) Law Enforcement S43(2) Commercial Interests
	2021.12.03 PCA DPIA Stage 2	S40(2) Personal Information S31(1) Law Enforcement S42(1) Legal Professional Privilege S43(2) Commercial Interests
	Community Impact Assessment	Released in full.
	Equality Impact Assessment	S23(1) Security Bodies
Question 3		
	2021.04.26 PDS Information Risk Assessment Report v 1.0 (PCA)	S23(1) Security Bodies S31(1) Law Enforcement S40(2) Personal Information S43(2) Commercial Interests
	2021.04.26 PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded doc 1)	S23(1) Security Bodies S31(1) Law Enforcement S40(2) Personal Information S42() Legal Professional Privilege S43(2) Commercial Interests

	2021.04.26 PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded doc 2)	S23(1) Security Bodies S31(1) Law Enforcement S40(2) Personal Information S43(2) Commercial Interests
	ICO Guidance on use of Cloud Computing (Embedded within PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded doc 2))	Withheld in full. S21
	Extract – points 49-51 of ICO Guidance on use of Cloud Computing (Embedded within PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded doc 2))	Withheld in full. S21
	Extract – point 98 of ICO Guidance on use of Cloud Computing (checklist) (Embedded within PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded doc 2))	Withheld in full. S21
	2021.04.26 PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded doc 3)	S23(1) Security Bodies S31(1) Law Enforcement S40(2) Personal Information S43(2) Commercial Interests
	2021.04.26 PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded doc 4)	S41(1) Information Provided in confidence S43(2) Commercial Interests
	2021.04.26 PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded doc 4 – Data Sharing Agreement)	Released in full.
	2021.04.26 PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded doc 5)	Released in full.
	2021.04.26 PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded doc 6)	Released in full.
	2021.04.26 PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded doc 7)	Withheld in full. S41(1) Information Provided in confidence.

	2021.04.26 PDS Information Risk Assessment Report v 1.0 (PCA) (Embedded doc 8)	Withheld in full. S31(1) Law Enforcement S41(1) Information Provided in confidence. S43(2) Commercial Interests
	IMORCC Embedded doc	S23(1) Security Bodies S40(2) Personal Information

Yours sincerely

Fiona Greenlees
NPCC Freedom of Information Officer & Decision Maker

www.npcc.police.uk

COMPLAINT RIGHTS

Internal Review

If you are dissatisfied with the response you have been provided with, in compliance with the Freedom of Information legislation, you can lodge a complaint with NPCC to have the decision reviewed within 20 working days of the date of this response. The handling of your request will be looked at by someone independent of the original decision, and a fresh response provided.

It would be helpful, if requesting a review, for you to articulate in detail the reasons you are not satisfied with this reply.

If you would like to request a review, please write or send an email to NPCC Freedom of Information, c/o PO Box 481, Fareham, Hampshire, PO14 9FS.

If, after lodging a complaint with NPCC, you are still unhappy with the outcome, you may make an application to the Information Commissioner at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Annex A

Legislation – Section 16

(1) It shall be the duty of a public authority to provide advice and assistance, so far as it would be reasonable to expect the authority to do so, to persons who propose to make, or have made, requests for information to it.

Legislation - Section 23 Information supplied by, or concerning, certain security bodies

(1) Information held by a public authority is exempt information if it was directly or indirectly supplied to the public authority by, or relates to any of the bodies specified in subsection (3)

This is an absolute exemption and there is no requirement to consider the public interest test.

Legislation - 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,

We acknowledge that there is a public interest in the disclosure of information concerning: the expenditure of public funds; the provision of services funded by the government; activities undertaken by policing and law enforcement; compliance with legal and regulatory obligations; and, measures undertaken to establish and maintain the confidentiality, integrity and availability of information.

Disclosure of this information would have the likelihood of identifying specific vulnerabilities, which would ultimately compromise police tactics, operations and future prosecutions. Any information identifying the focus of policing activity could be used to the advantage of criminal organisations. Information that undermines the operational integrity of these activities will adversely affect public safety and have a negative impact on law enforcement. Public safety would be put at risk if criminals were able to counteract police tactics.

The NPCC is committed to demonstrating proportionality and accountability. We consider that there is a weighty public interest in protecting from disclosure details of police and/or wider law enforcement methods which could assist offenders to avoid or evade detection, thus prejudicing the prevention or detection of crime, the apprehension or prosecution of offenders, the administration of justice and the exercise by a public authority of its functions.

We also consider that there is a strong public interest in protecting police and law enforcement systems, networks and devices from unlawful reconnaissance and attack contrary to the Computer Misuse Act 1990 and therefore in withholding from disclosure any information which could serve to make them more vulnerable to such illegal activities which would severely inhibit the ability to prevent or detect crime. Furthermore, it is appropriate to consider the wider implications of disclosure, including the social and financial cost that would be necessary to attempt to mitigate the adverse impact of the prejudice that would, or would be likely, to occur and that these would require the re-prioritisation of resources, which would not be in the public interest.

Balancing the competing public interests, we note that information already in the public domain, such as on the Police CyberAlarm website, together with the information being disclosed in response to your requests (including confirmation that relevant assessments have been undertaken) contributes to meeting the public interests identified above which would favour the disclosure of the requested information. We further note that the activities undertaken by police and law enforcement in relation to Police CyberAlarm are already subject to established legal and regulatory frameworks and associated scrutiny. Conversely, as the Information Commissioner has recognised, *"There is a very strong public interest in protecting the ability of public authorities to*

enforce the law". We do not consider that the prejudice that would, or would be likely to occur, as a result of disclosure could be eliminated by other means. Consequently, we consider that the public interest favours maintaining the exemption and withholding the requested information in so far as s31 FOIA applies.

Legislation - Section 40 Personal Information

(1) Any information to which a request for information relates is exempt information if it constitutes personal data of which the applicant is the data subject.
(2) Any information to which a request for information relates is also exempt information if
(a) it constitutes personal data which does not fall within subsection (1), and
(b) the first, second or third condition below is satisfied.

(3A) The first condition is that the disclosure of the information to a member of the public otherwise than under this Act—
(a) would contravene any of the data protection principles, or
(b) would do so if the exemptions in section 24(1) of the Data Protection Act 2018 (manual unstructured data held by public authorities) were disregarded.

(3B) The second condition is that the disclosure of the information to a member of the public otherwise than under this Act would contravene Article 21 of the GDPR (general processing: right to object to processing).

Any information to which a request for information relates is also exempt information if it constitutes personal data which do not fall within subsection (1), and either the first or the second condition is satisfied.

S40(2) applies to third party personal data. Any release would breach the data protection principles contained within the Data Protection Act 2018. S40(2) has been engaged by virtue of S40(3)(a)(i).

Where the request captures personal informational including third party personal data, it is an absolute exemption under section 40(2) if disclosure would breach any of the data protection principles.

Any disclosure of withheld information would breach the first data protection principle of fair and lawful processing. This is an absolute exemption and there is no requirement to apply the public interest test.

Legislation - Section 41 Information Provided in Confidence

(1) Information is exempt if –
(a) It was obtained by the public authority from any other persons (including another public authority), and
(b) The disclosure of the information to the public (otherwise than under this Act) by the public authority holding it would constitute a breach of confidence actionable by that or any other person.

This is an absolute exemption and there is no requirement to consider the public interest test. In this case, this applies to recorded information disclosed by the supplier in the course of the procurement process, and also to an independent external security assessment commissioned by the supplier.

Legislation - Section 42 Legal Professional Privilege:

(1) *Information in respect of which a claim to legal professional privilege or, in Scotland, to confidentiality of communications could be maintained in legal proceedings is exempt information.*

Legal professional privilege (LPP) protects confidential communications between lawyers and clients: it is a fundamental principle in English law.

The client's (NPCC) ability to speak freely and frankly with their legal adviser in order to obtain appropriate legal advice is a fundamental requirement of the English legal system.

The concept of LPP protects the confidentiality of communications between a lawyer and client. This helps to ensure complete fairness in legal proceedings. On this occasion, this information relates to the advice privilege which applies where no litigation is in progress or contemplated. It covers confidential communications between the client and lawyer, made for the dominant (main) purpose of seeking or giving legal advice.

The public interest in maintaining the legal professional privilege that exists between client and solicitor cannot be undermined and because there has not been any prior legal advice or published advice and therefore outweighs the public interest in disclosure.

The Information Commissioner has emphasised that *"The general public interest inherent in this exemption will always be strong due to the importance of the principle"* of legal professional privilege. Weighty factors are therefore required in order to tip the balance in favour of disclosure. While acknowledging the public interests identified above and the general public interest in transparency, in the circumstances we do not consider that these outweigh the significant public interest in maintaining the exemption.

The legislation - Section 43 Commercial Interests

(2) Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice commercial interests of any person (including the public authority holding it).

Section 43 has been relied upon where disclosure of the requested information would, or would be likely to, prejudice the commercial interests of the public authority, the supplier and/or third parties.

We are mindful of the contribution to the recognised public interest in the expenditure of public funds and provision of government-funded services offered by the information disclosed in response to your requests, as well as information already in the public domain such as information pertaining to the procurement of Police CyberAlarm (see https://ted.europa.eu/udl?uri=TED:NOTICE:236115-2020:TEXT:EN:HTML and https://ted.europa.eu/udl?uri=TED:NOTICE:236115-2020:TEXT:EN:HTML) and responses provided to previous requests under FOIA for information concerning Police CyberAlarm.

We note that the supplier had specifically identified some of the requested information as being liable to cause it commercial prejudice in the event of its disclosure during the procurement process. We are also concerned about the prejudice that would be caused to the supplier by the asymmetric disclosure of its commercially sensitive information when other parties to the procurement process - and indeed other competitors - would not suffer the same disadvantage.

We also reflect on the additional costs to the police, wider law enforcement, the supplier and other third party providers in the event of the disclosure of information which could assist offenders or leave networks, systems and devices more vulnerable to attack, both in terms of seeking to defend against or deploy mitigations, and to remedy a successful attack. In the circumstances, we are satisfied that the public interest favours maintaining the exemption and withholding the requested information in so far as s43(2) FOIA applies.