The Gryphon Trust

DPIA Police CyberAlarm Notice

POLICIES AND PROCEDURES PROFORMA

Subject	DPIA Police CyberAlarm Notice
Version	1.0
Author	Miss Milligan, IT Manager
Persons / Committees consulted whilst document in draft	Headteachers Governing Body
Date Policy Agreed	March 2022
Date of Next Review and By Whom	September 2024 IT Manager
Copy obtainable from and / or distribution	PA to the Headteacher
Date Document Issued	February 2022
Responsibility for Dissemination to New Staff	Line Managers
Policy Review	Biennially
Headteacher Target Audience	All Staff All Students Parents Commissioning Schools Local Authorities

Amendments Summary:

Amend. No.	Issued	Page	Subject

Name of System

Police CyberAlarm

1.0 Aims of System

Police CyberAlarm identifies suspicious activity as network traffic which is blocked by the member organisations firewall or that is believed to be unwanted. This will include activity where the suspect is attempting to scan for vulnerable ports or making repeated attempts to gain access to an organisation's system using known attack methods.

By monitoring this data at our schools, we can be quickly alerted to any suspicious activities from our networks, which will add to the range of tools we have in place to keep our systems and data as secure as possible.

2.0 Personal Data Used by System

Police CyberAlarm collects metadata (logs) relating to the suspicious activity from internet facing gateways such as Firewalls. They are simply logging about how data was sent/received through the schools' internet gateway (IP Addresses for external connections, amount of data transferred and the port used to process the data, date and time).

The personal data collected and processed in connection with the deployment of the Police CyberAlarm tool will include personal data, special category personal data and criminal conviction and offence data.

Personal data collected from the school will be comprised of:

- Online identifiers, such as IP address, relating to suspicious firewall activity; and
- Conduct data, i.e. information relating to the conduct which led to it being identified as being suspicious firewall activity.

This personal data relates to people suspected of committing an offence.

Data pertaining to suspicious firewall activity will be collated, analysed and may be matched against other data sources. Where an investigation is launched into suspicious firewall activity, further personal data may be sought and collected, which may include special category data, and this will take place in accordance with the relevant law enforcement agency's own privacy policy.

Police CyberAlarm reports summarise suspicious traffic and potential attacks, visible to the school from the Internet. Details include the top sources of suspicious traffic and the ports that malicious users are trying to use for their attacks against your systems.

The data is split into two categories, suspicious activity originating from within the UK and suspicious activity from outside the UK.

Police CyberAlarm reports show the school how they are being attacked, and where from, so the school can better protect themselves.

3.0 Purpose of Processing

The school will rely on 'public task' as their lawful reason to process data.

4.0 Steps Taken by Police CyberAlarm to Protect Data

Sharing data:

- The data collected by Police CyberAlarm is viewable only by Police and may be shared with other law enforcement agencies including the NCA (National Crime Agency) and partners including the NCSC (National Cyber Security Centre).

- Additionally, they may also share your data with the following:

    - Police Forces in Great Britain and Northern Ireland;
    - Their third-party service providers; and
    - Professional advisors.

Restrictions:

- Only communications data pertaining to suspicious activity will be collected and, to the extent that any data is mis-identified, this will not be stored and will be erased as soon as possible. Restrictions will be imposed in relation to the use of data collected to ensure compliance with legal obligations.

Retention:

- Logs collected by Police CyberAlarm are analysed by the collector as they are received, to remove any obviously non-malicious logs, these events are not sent to the central server. Once logs arrive at the central server, they are analysed within minutes (even seconds) of the event being received by the collector to determine if these logs are malicious.

    - For example, a log which is a request to connect using port 3389 may be deemed as non-malicious. However, if the central server correlates that the same IP address made rejected requests to port 3388, 3387, 3386, etc. then this would become part of a potentially malicious port scan.

- Any log which, following analysis, at both the CyberAlarm Virtual Server and the Central Server is still deemed to be non-malicious within a maximum of 24 hours (system up time) within arrival at the Central Server will be removed.
- If a log file which has been deemed as suspicious has no further linked activity within a 9-month period the relevance of the data is reduced and its retention is no longer considered to be necessary or proportionate and as such is deleted.

Reasons to install onsite:

- The log messages from internet facing devices are not encrypted. To ensure security Police CyberAlarm system installs a small collector on your network. Typically, this would be installed within your DMZ to gather the data from suspicious and /or malicious traffic. The data is then encrypted and compressed before being securely transmitted to the CyberAlarm central processing servers. It will not be installed on every device. Police CyberAlarm is a stand-alone system which sits in its own server environment. The collector gathers and encrypts the suspicious data from your internet gateway before sending it back to the central Police CyberAlarm processing servers. No software need be installed on any other devices and multiple gateways can feed data to a single Police CyberAlarm collector.
- Police CyberAlarm is a monitoring system and as such does not interfere with any of the traffic on your internet gateways.
- Police CyberAlarm does not take any automated action against any identified suspicious activity. It is a reporting and alerting system only, which enables UK Police to identify and act against cyber threats and allows member organisation to better inform their cyber security posture.
- Responsibility for decisions on how to action any reported data is solely owned by the school.

Transferring Data:

- Data on the Police CyberAlarm data collector is compressed and encrypted on the collector (256bit AES), then uploaded to the Police CyberAlarm servers over HTTPS, an encrypted web connection.
- Personal data is not routinely transferred outside the EEA in connection with Police CyberAlarm.

5.0 Steps Taken by School to Protect Data

The Schools will only have the CyberAlarm installed in one location at each school which will be able to provide enough access for this service to work. Where CyberAlarm is installed, the systems will be kept up to date with full Anti-Virus software running alongside it and all security patches applied promptly after their release, in a bid to keep the CyberAlarm logs safe.

The schools will further lock down the logs to only be accessible from the IP addresses/range of the Police CyberAlarm service, reducing the risk of unauthorised access to this data.

6.0 Impacts and Risks

School Assessment of Risk		
	Risk Level	Comments
Likelihood of harm	Unlikely	The data is encrypted and kept on secure systems
to data subject		with limited access to them
Severity of harm (regardless	Significant	The personal data may contain criminal conviction
of likelihood)		or offence data and therefore special category data
Overall risk (considering	Medium	Despite the severity of harm being significant it is
measures to reduce risk above)		unlikely of any harm to the data subject therefore we place the risk at medium
DPO Assessment of Risk		
	Risk Level	Comments
Likelihood of harm	Unlikely	
to data subject	Possible	
	Likely	
Severity of harm (regardless	Minimal	
of likelihood)	Significant	
	Severe	
Overall risk (considering	Low	
measures to reduce risk above)	Medium	
	High	

7.0 Compliance Statement

I can confirm that this data protection impact assessment has been completed to the best of my knowledge and that the technology complies with the data protection principles under the GDPR.

All privacy risks and solutions have been considered and represent a proportionate response to the identified risks to personal data