



REPORT TO THE POLICE SERVICES BOARD

Author: Teresa Fetter. Director Business Services

Date of Report: 11/15/2022

Type of Report: Public

Title: Asset Protection

RECOMMENDATION

THAT the Board finds that all provisions of the *Asset Protection Executive Limitations* policy has been complied with.

I hereby submit my monitoring report on your Executive Limitations Policy, “Asset Protection” according to the schedule set out. I certify that the information contained in this report is true.

BROADEST POLICY PROVISION:

The Chief of Police will not cause or allow Durham Regional Police Service assets to be unprotected, inadequately maintained or unnecessarily risked.

Interpretation of the Chief of Police:

It is my interpretation that the Board has comprehensively interpreted this policy in its subsequent policy provisions. My interpretations will be attached to those provisions below.

Further, without limiting the scope of the foregoing by the enumeration, the Chief of Police will not:

Policy Provision #1

1. “Unnecessarily expose the organization, its members, the Board or the Regional Municipality of Durham to claims of liability.”

Interpretation of the Chief of Police:

Policing involves activity by our members in which they place themselves in danger as well as our tangible and intangible assets at risk of loss or damage.

I will take all reasonable steps to ensure that the Service is managed and controlled with an attitude, systems and procedures which avoid these outcomes. The Risk Management Committee takes a proactive approach to monitoring and reporting on major risks.

Claims of liability means lawsuits launched by parties who allege that they have been damaged by the actions of our members in the course of their duties.

I interpret unnecessary exposure to such claims to occur when our members knowingly take actions or allow conditions to occur which will likely result in a claim.

Further, in view of the fact that some claims will succeed even if all actions are proper, I will ensure that the insurance arrangements put in place by the Region of Durham provide an adequate level of protection against claims which are made.

Data in Support:

Risk Management Committee

1) Mandate and Definition

“To develop a systematic approach to identifying, monitoring and reducing risks affecting human life and health, reputation and property.”

Our definition of risk management is “the process of looking into the future for things which may go wrong and doing something now to prevent them going wrong or lessen the damage of those things going wrong.”

Our focus is activities which can be examined and improved to lessen unnecessary risks.

2) Committee Membership

The Committee is chaired by the Director of Business Services and is composed of the Unit Leaders or ELT representatives from our Quality Assurance Unit (policies and procedures, risk based audits), Strategic Planning Unit, Professional Standards Unit (police discipline and Special Investigations Unit liaison), Legal Services Unit (civil claims), Police Education and Innovation Centre (training), Superintendent of Policing Operations and Duty Inspectors’ Office (front-line operations and Police Vehicle Operations Safe Arrival Committee).

3) Standing Reports

Currently consist of:

- Vehicle Collision report produced by Fleet Management and posted monthly to the Service’s intranet site,
- Police Vehicle Operations Safe Arrival Committee update produced by the Duty Inspector – Quality Assurance,
- Public and Internal Complaints report produced by the Professional Standards Unit,
- Special Investigations Unit Incident report produced by the Professional Standards Unit,
- Lawsuit Update report produced by Legal Services,
- A Use of Force report produced by the Police Education and Innovation Centre, and
- An audit report produced by the Quality Assurance Unit.

Vehicle Collisions

Driving vehicles is the single riskiest activity in which police officers engage, based on both its frequency and the negative consequences of collisions.

The Risk Management Committee has helped the service focus on reducing our vehicle collisions and the attendant injuries:

Departmental Collisions Injuries and Expenses				
	2020 Year	2021 Year	2021 Sept. YTD	2022 Sept. YTD
Member Injuries	10	7	7	13
Time Lost in Hours	1369	2820	460	442
Wages Lost(Straight Time)	\$74,295	\$135,254*	\$22,614	\$19,043
WSIB Non-Wage Expenses	\$27,322	\$34,533	\$4,578	\$1,500
# of Collisions	117	127	99	103
# Write-Offs	16	4	3	5
Average Repair Cost	\$6,914	\$5926	\$6,297	\$5,288
DRPS Collision \$ Value	\$808,923	\$752,649	\$623,392	\$544,708

** the increase to the 2021 Year result is due to the significant length of time lost for a few members*

Suspect Apprehension Pursuits

Suspect apprehension pursuits are governed by the Durham Regional Police Service (DRPS), Directive **LE-10-001 “Suspect Apprehension Pursuits”**. The directive contains stringent policies and procedures for frontline officers to adhere to when during their regular tour of duty, they are confronted by the unlawful actions of a motorist in making a decision to engage in a suspect apprehension pursuit, continue or discontinue the pursuit, and terminate the pursuit. The DRPS policy follows the guidelines provided by the Ministry of the Solicitor General Policing Standards Manual (2000), Law Enforcement Standard # LE-045.

The table below provides the number of suspect apprehension pursuits engaged in by DRPS officers for the full year in 2020 and 2021 and, year-to-date for 2021 and 2022:

Suspect Apprehension Pursuits	2020 Year	2021 Year	2021 Sept. YTD	2022 Sept. YTD
Number of Pursuits	135	140	107	94
Compliant	127 (94%)	132 (94%)	100 (93%)	88 (94%)
Non-Compliant	8 (6%)	8 (6%)	7 (7%)	6 (6%)

DRPS has been capturing pursuit data since 1996. The Service has seen the trend on the number of pursuits range from a high of 140 (2021) to a low of 32 (2012). The regulation sets out a **three-part** test that must take place before a police officer may undertake a suspect apprehension pursuit. This directly affects the frequency of pursuits occurring during a given year. The bottom line is public safety which includes not only vehicular and pedestrian traffic, but also occupant(s) of suspect vehicle and the primary officer engaged in the pursuit.

It is worth noting that most pursuits are less than 5km and take less than 2 minutes. Each pursuit is debriefed by the Duty Inspector on duty at the time of the pursuit and officers involved to assess both directive and Ministry compliance.

Compliance with the DRPS suspect apprehension pursuit policy is also closely monitored by the Pursuit Review Officer within the Quality Assurance Unit. The Pursuit Review Officer reviews all material related to a suspect apprehension pursuit as soon as is practicable after the pursuit has been reported. This close scrutiny ensures that any deviations from policy or procedures can be quickly addressed and corrected.

The compliance rate with the pursuit directive has steadily increased due to the training, debriefs and officer actions. The years 2020 and 2021 witnessed the highest level on record at 94%.

Based on the data, the risk is being diligently managed with exceptional results in this activity.

Special Investigations Unit (SIU) – 2020 to Present

In **2020**, the SIU invoked their mandate on ten (10) incidents involving our members with the following results:

- In three (3) of the cases, the SIU decided not to proceed and terminated its investigation.
- In six (6) of the cases, the subject officer was cleared of criminal responsibility by the SIU. The subject officer was also found by the Professional Standards Unit not to have committed any offence under the Code of Conduct of the *Police Services Act*.
- In one (1) case, the subject officer was charged criminally by the SIU and was later withdrawn.

In **2021**, the SIU invoked its mandate on fifteen (15) incidents involving our members with the following results:

- In four (4) of the cases the SIU decided not to proceed and terminated their investigation.

- In ten (10) of the cases, the subject officer was cleared of criminal responsibility by the SIU. The subject officer was also found by the Professional Standards Unit not to have committed any offence under the Code of Conduct of the *Police Services Act*.
- In one (1) case, the subject officer was charged criminally by the SIU. The criminal charge was withdrawn and a Bylaw Infraction was laid.

Comparison

From **January 1st 2021** up to and including **September 30th, 2021**, the SIU invoked its mandate on eleven (11) of our members with the following results:

- In three (3) of the cases the SIU decided not to proceed and terminated their investigation.
- In five (5) of the cases, the subject officer was cleared of criminal responsibility by the SIU. The subject officer was also found by the Professional Standards Unit not to have committed any offence under the Code of Conduct of the *Police Services Act*.
- In one (1) case, the subject officer was charged criminally by the SIU and the case is still before the courts.
- The other two (2) cases were still under investigation by the SIU at that time and a decision had not yet been rendered.

From **January 1st 2022** up to and including **September 30th, 2022**, the SIU invoked its mandate on eight (8) of our members with the following results:

- In four (4) of the cases, the subject officer was cleared of criminal responsibility by the SIU. The subject officer was also found by the Professional Standards Unit not to have committed any offence under the Code of Conduct of the *Police Services Act*.
- The other four (4) cases are still under investigation by the SIU and a decision has not been rendered.

Civil Liability Claims

The following chart provides a breakdown of civil liability claims, by category, for the past two years:

Year	Assault/Excessive Use of Force	Departmental MVC	Unlawful Arrest	Improper Search and Arrest	Malicious Prosecution	Negligence	Total
2020	1	0	2	0	0	6	9
2021	0	2	1	0	1	4	8

The following chart provides the comparison of civil liability claims received from January 1st to September 30th in 2021 and 2022:

Sept YTD	Assault /Excessive Use of Force	Departmental MVC	Unlawful Arrest	Improper Search and Arrest	Negligence	Wrongful Arrest	Charter Breach	Total
2021	0	1	0	0	4	0	0	5
2022	0	1	0	0	6	1	1	9

Each year, the Region of Durham’s Manager of Risk and Insurance and the Commissioner of Finance attend an in camera meeting to provide the Board with a confidential overview of Risk Management and claims experience as it relates to the Service.

Insurance Coverage

The Regional Finance Department's Insurance and Risk Management Division manages the insurance program which provides protection for individuals and assets along with protection against liability. Further protection is provided for claims made against the Service, its members, the Board and the Region. This program includes comprehensive policy wordings with high limits of liability. The Region has assured us that they have developed comprehensive custom solutions that will meet the Service’s needs.

Statement of Compliance/Non-Compliance:

I report compliance with this provision.

Policy Provision #2

2. “Fail to report to the Board the details of any claims settled or awarded in the amount of \$250,000 or more, as soon as possible following the settlement or award”.

Interpretation of the Chief of Police:

It is my interpretation of the provision that I am to ensure that the Region’s Risk Managers provide the requisite report to the Board.

Data in Support:

Year	Civil Settlements or Awards exceeding \$250,000
2020	0
2021	0

In comparing civil settlements or awards exceeding \$250,000 from January 1st to September 30th in 2021 and 2022, the results are as follows:

Sept YTD	Civil Settlements or Awards exceeding \$250,000
2021	0
2022	0

Statement of Compliance/Non-Compliance: I report compliance with this provision.

Policy Provision #3

3. “Fail to protect intellectual property, information and files from loss, damage or compromise.”

Interpretation of the Chief of Police:

It is my interpretation of the provision that I am to ensure there are effective systems and controls to protect intellectual property and information, and that patents and licensing provisions of electronic information and systems remain secure from breaches, misuse or misappropriation. Furthermore, I have a duty to ensure that the intellectual property licensed by the Service and developed for the Service is protected.

Data in Support:

Human Resources Policies on Intellectual Property Protection

In relation to protecting the development of intellectual property while in the employ of, or on behalf of the Service, Human Resources ensures that all offers of employment clearly identify the proprietary rights of the Service for the intellectual property and products developed on behalf of the Service, during the individual’s term of employment (contract or otherwise). There are also directives in place to deal with installation of hardware and software as well as monitoring tools to determine if there is inappropriate software installed on our network.

The Human Resources unit has confirmed that new employees of the Service are required to sign an employment offer letter agreeing to abide by the Service’s Intellectual Property policy which reads as follows:

“Intellectual Property

All work products including documentation, reports, and intellectual property created or developed by the member for the DRPS during the course of their employment shall belong to and remain with the DRPS.”

Information Technology Policies on Database Security

Directives include:

AO-08-005 “Computer Data Recovery and Data Storage Management”

AO-08-001 “Internet Use by Police Service Members”

AO-08-003 “Electronic Messaging (e-mail and VMDT transmissions)

AO-08-002 “Computer Software and Hardware”

AO-08-006 “Automatic Vehicle Locator”

The I.T. Unit supports over 19 buildings and has over 300 physical and virtual servers, 900+ workstations, 400+ laptops, 550+ smartphones, over 600+ applications and 1500+ members and non-members accessing our network. In addition to the hardware /software and users that we

support, we have multiple domains, multiple workgroups and a multilayered network that would need to be recreated in order to return to normal operations, in the event of a Cyber Attack

Since the pandemic and shift to the hybrid model, Cyber Security is one of the main trends globally for all organizations and Durham Regional Police is no exception and with an extensive amount of network security products available to us these tools help to prevent zero day attacks on our users, apps and servers and we connect and secure all of our end points. This includes our corporate networks, our data centers (All divisions), any SaaS (Software as Service) systems, Internet sites like drps.ca, any of our managed devices, our smartphones which includes VPN software and various other IoT devices/BWC etc.

The IT department has an extensive list of security tools in place for endpoint protection which consist of threat extraction, threat prevention, endpoint anti-virus, firewalls, intrusion preventions and various network auditing tools.

Daily/Weekly/Monthly and Yearly security audits includes all of the end point protections on all of our hardware and software systems. These products include the following:

- **Check Point:** Next Generation Threat Prevention Blades, Threat Extraction Package software, Threat Prevention & SandBlast (NGTX), Endpoint Anti-Virus renewal
- **CISCO IrontPort** –A security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. Helps with Zero Day threats
- **Imperva Sonar** - DRPS.CA for web site protection includes DDoS Protection, Advanced BOT protection and more.
- **Vectra Cognito Cloud Protect O365**- Review of O365 SaaS applications federated with Azure AD.
- **ManageEngine OpManager**-, end-to-end network management software on advanced fault and network performance management functionality across DRP's network devices via the WAN
- **CheckPoint** NG Firewalls with redundancy
- **CISCO routers/switches** with endpoint security software installed

The Infrastructure security audit tools alerts our security team and or networking teams of any potential threats/hacks or attacks to our network or devices. However, even with the greatest tools in place the best strategy to protect our systems and users against social engineering (defined as the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques) is awareness of the risk.

Other methods for Protection included within IT are the following:

- **DRPS security patching:** Outdated software or existing vulnerabilities in various applications might be fertile grounds for malware attacks. IT does regular patching which helps prevent Advanced Persistent Threats (APTs).

• **Application whitelisting** is a form of application control that takes a trust-centric approach of allowing only the known good. Essentially, DRP IT Security team provides authorization and granted only to applications, files, directories, or processes that are classified as required and safe to execute. Everything else denied by default. Application whitelisting is done using attributes like file name, file size, and/or directory path.

• **Application blacklisting** is a simple and straightforward security strategy where everything that is known to be malicious – the known bad – is prevented from running on our DRP endpoints and servers that are part of the network. Blacklisting takes a threat-centric approach to block all possible malicious software from taking hold of the network. It is a list of signatures and hashes that have been deemed malicious or suspicious and are therefore prevented from being downloaded or executed on your systems. The software we purchased does this automatically.

• **Up-to-date anti-malware/antivirus with Checkpoint/CISCO IronPort:** First line of defense is our antivirus program that proactively and automatically scans our DRP systems and networks on a regular schedule for any malware software.

• **Remote device encryption:** VPN Checkpoint Endpoint Encryption was implemented for data encryption protection on our DRP smartphones, Laptops and PCs. Specifically accessing our networks remotely since we work from home and the hybrid workplace is the “new normal.”

• **Access protection:** This ransomware protection hygiene includes network firewalls (Checkpoint), (CISCO router protection), strong password policy, and multi-factor authentication with PKI and also SMS.

• **Education:** Security awareness for our members is conducted on a regular basis through various forms of communications (What’s new, All, Mediaone SharePoint). There is an FAQ and Security Awareness site on Mediaone.

Overall, there have been no instances that I am aware of where intellectual property, information or files have been lost, damaged or compromised. However, we do conduct reviews on member’s emails, MDT’s, CCTV private files and GPS records when required by the Professional Standards Unit or senior command relating to a particular incident or case. Unit leaders are requested to fill out the following e-Forms for any non-compliance of our directives that take place.

- CCTV Hide e-Form – DRP 112
- Internet, Email, Secure Folder Audit DRP 209H
- GPS Audit – DRP209F
- Private/Invisible RMS – DRP140

Number of audits conducted in 2022:

- 1) Internet/email - 8 audits were conducted
- 2) Total RMS Audits - 153 Private and 31 Invisible Requests
- 3) CCTV hidden requests - 155 requests

There are also strict provisions that limit the utilization of licensed products (e.g. computer software), which are strictly monitored and managed by our Information Technology Department, including the administrative controls over adding computer programs and the downloading of programs.

The Information Technology unit purchased a third-party service to assist in cybersecurity protection of our DRPS website. The service is called Imperva and it provides an extra layer of protection to our drps.ca site to deal with security threats and vulnerabilities that hit our site daily. It works at scrubbing and processing up to 30 billion attack packets per second. Imperva also defends our web site against attacks and provides added protection for DDoS attacks. It also conducts IP masking which prevents direct to IP DDos attacks by hiding the IP from our original server for added security protection.

**Statement of Compliance/Non-Compliance:
Therefore, I report compliance with this provision**

Policy Provision # 4

4. “Receive, process or disburse funds and found or seized property under controls that are inconsistent with sections 132, 133 and 134 of the Police Services Act, or insufficient to meet the standards of the auditor appointed by the Regional Municipality of Durham.”

Interpretation of the Chief of Police:

It is my interpretation of this provision that I am to ensure that appropriate directives and procedures are in place to meet the above standards and that they are being complied with. The directive covering these procedures is in place and is called AO-04-001 Seized and Found Property. The Quality Assurance Unit is required to complete a yearly audit as per our internal directives.

Data in Support:

Directive AO-04-001 Seized and Found Property addresses the management, storage and disposition of personal property, money and firearms, which come into the possession of the police service in accordance with sections 132, 133, and 134 of the Police Services Act. The directive is to be reviewed within three years of the last review date and updated as necessary; it was most recently updated in August 2019 and is now due for a full review.

Quality Assurance completed an audit of the property control function in June 2021. The audit tests the accuracy of the records relating to property and evidence. The result of the audit is reported to the Board in the Audit Function Monitoring Report each year. An inspection of the divisional property control function is scheduled for this reporting year. (M130-22 refers).

**Statement of Compliance/Non-Compliance:
Therefore, I report compliance with this provision.**

Policy Provision # 5

5. “Fail to ensure that all monies that accrue from the local sale of unclaimed goods are promptly transferred to the Board’s control.”

Interpretation of the Chief of Police:

It is my interpretation that I shall ensure that all revenue accrued from the sale of unclaimed goods is accounted for, and that all monies from the sale are properly and promptly transferred to the Board.

Data in Support:

The Property unit arranges public auction sales with an independent web-based online auctioneer, pursuant to a formal agreement. Both the Unit and the auctioneer maintain separate records of the sales and funds received.

The DRPS is provided a record from the auctioneer that details each item sold, the amount of the bid, and the final bidder. As the online auction is continuous, on about a monthly basis Property staff conduct a reconciliation of the auction list and property files, and the remitted funds are sent to the Board. There are no known discrepancies between the records and the amount remitted.

The auctioneer provides the Durham Regional Police Services Board with a cheque for the proceeds minus their commission. The Service has no role in remitting funds other than to act as courier of the cheque to the Board. The records provided by the auctioneer are kept on file in the Property Unit in accordance with retention by-laws.

Auction reconciliation has been completed up to and including items sold in July 2022. As of September 30, 2022, the cheque for the May 2022 auction sales was outstanding due to the disruption by the fire at Courtice Court. The Property Unit has been in contact with the auctioneer regarding this matter and it is expected a replacement cheque will be received by November 2022. Although records indicate the auctioneer is in possession of 195 items yet to be sold, some dating back to 2019, we anticipate there will be fewer items added to the auction inventory due to fire loss.

Statement of Compliance/Non-Compliance:
Therefore, I report compliance with this provision.

Policy Provision # 6

6. “Compromise the independence of the Board’s audit or other external monitoring or advice. Engaging parties already chosen by the Board as consultants or advisers is unacceptable.”

Interpretation of the Chief of Police:

It is my interpretation of this provision that I will not engage parties who are under contract to the Board where a conflict of interest may exist or where it may compromise the independence of the Board's audit or other external monitoring.

Data in Support:

I have been provided a list of these parties by the Executive Director of the Board. I confirm that the Service has not taken any actions with these parties which would compromise the independence of these parties as it relates to providing advice or monitoring to the Board.

The list of parties is as follows:

In 2021: Perley-Robertson, Hill and MacDougall; Deloitte and Touche; Graymatter Marketing - Media; Environics Research; Delta One and Associates; Escribe

January 1, 2022 up to September 30, 2022: Perley-Robertson, Hill and MacDougall; Deloitte and Touche; Environics Research; Graymatter Marketing – Media; Delta One and Associates; Clunis Consulting; Waterhouse Executive Search; Escribe

Statement of Compliance/Non-Compliance:

Therefore, I report compliance with this provision.

Policy Provision # 7

7. “Endanger the organization’s public image, credibility or its ability to accomplish Ends.”

Interpretation of the Chief of Police:

It is my interpretation of this provision that the Service will not perform any action that impacts negatively on the public image or credibility of the Police Service. The Service will not perform any function that is contrary to the achievement of the Board's Ends.

Data in Support:

Corporate Communications provides both proactive and reactive support in managing the integrity of the Service and its brand. It does this through various means that include:

- Strategic communication advice to Command, the Executive and Senior Leadership Teams and others in the service to prevent and manage situations that could lead to negative brand sentiment.
- Proactive community engagement through stories and videos highlighting the great work of DRPS and its members.
- Supporting and working with stakeholders on events and issues.
- Producing media releases and media management.
- Assessing and identifying new ways to communicate with our stakeholders

- Creating public service and educational communications to better serve our community.

Traditional media and social media coverage have a direct impact on how the public perceives the police service. Additionally, the public does not see the majority of work we do and therefore might not understand when we are patrolling their community, the vast majority or proactive community policing, our responses to urgent and emergency calls and the investigative work we do.

Durham Region has far less traditional media outlets than it did 20 years ago and those media companies have greatly reduced staff and coverage. While we continue to work with our local and Toronto media stakeholders to provide timely responses to their inquiries, we continue to use our own social channels to push out content and keep our public informed.

That said, the organization's image and reputation remained positive in 2022, based on media/social media measurements done by the Corporate Communications Unit.

The unit remained dedicated and active throughout the year sharing positive news stories and social media posts on a daily basis with the public and the media. The Unit was diligent in exploring new ways to expedite information including the introduction of Twitter Releases over more traditional and time-consuming processes. While certain events require full media releases, the Twitter Releases were well received by the media. The Unit, and specifically Acting Sgt. George Tudos, continue to be diligent in responding to media and has a strong working relationship with the traditional media outlets.

(Note - For all social media data YTD refers to Sept. 30, 2022)

In 2021, the Unit issued 609 formal media releases; down from the 630 issued in 2020. So far in 2022, the Unit has issued 388 media releases, which is down from the 490 issued at this time last year. That change is connected to the service using social media more especially in cases that are timely like missing persons. Our ability to get attention and traction from media and community actually comes from social media.

In addition to traditional media releases, the Unit issues Twitter Releases and issued 92 of these new social media releases in 2021. So far, in 2022, the Unit has released 36 Twitter releases. Recognizing Twitter as an important resource for direct communication with the public, and that not all information we disseminate has to be in the form of a media release we have been posting more time sensitive updates directly to social media without a formal release. So far in 2022 (as of Sept. 30), the Corporate Communications Unit has issued 1,332 tweets. In all of 2021, 1575 tweets were issued.

DRPS began sharing information on its official social media channels in 2012 via Facebook and Twitter. In 2019 DRPS started an Instagram account.

Last year at this time we had 76,299 followers on Twitter and that has increased to 88,163 in 2022 (as of Sept. 30) – a significant increase of almost 16 per cent.

In 2021 we had 48,895 followers on Facebook, which has grown to 55,000 in 2022 year-to-date – an increase of nearly 13 per cent. What was not always measured, and is a more important metric, is Page Reach – the number of people who saw content from our Facebook page. In 2020 our

Facebook page views were 1.95 million. In all of 2021, we had 2.75 million page views. Year-to-date in 2022, we are at 2.14 million page views.

DRPS launched an Instagram account on May 9, 2019 and has seen its followers grow from 8,547 in 2021 to 10,382 followers in 2022 year-to-date. Page reach is also an important metric on Instagram. In 2021, our Instagram page reach was 44,560 and so far, in 2022 it is 46,382.

Since 2018, the DRPS YouTube channel has grown to 1.61 million views (up from 1.5 million in 2021) and 2,730 subscribers (up from 2,300 in 2021). DRPS shares most of our videos directly on Facebook/Instagram and Twitter and not posting all content to YouTube.

Overall, activity and engagements across all of our social media platforms has increased in 2022 compared to 2021. Total impressions (the number of times a post on one of our social media channels was seen) for 2021 (Jan-Oct) was 25.7 million. Year-to-date in 2022 our impressions are 40.9 million – a substantial increase of 59 per cent.

In 2021, the Corporate Communications Unit began using a new media monitoring service to ensure we were capturing all of the media coverage. From Jan 2021 – October 2021 DRPS had 24.3K news mentions with 10.6 billion impressions. Year-to-date in 2022, DRPS has 43.4K news mentions with 11.3 billion impressions.

The vast majority of news articles/editorial monitored in 2022, were positive or neutral in tone about the police service and some were negative in tone.

The issues contributing to a majority of the negative media coverage in 2022 included:

- Courtice Court Fire and damage to property and criminal evidence
- Constable Erin Howard video in support of the Ottawa Trucker Convoy and subsequent Police Standards hearings.
- Hells Angels hold meeting at chapter in Brooklin

**Statement of Compliance/Non-Compliance:
Therefore, I report compliance with this provision.**

Policy Provision # 8

8. “Change the organization’s name or substantially alter its identity in the community.”

Interpretation of the Chief of Police:

It is my interpretation of this provision that there will be no change in the name of the Service or in the role that the Service plays within the community.

Data in Support:

I have neither directed nor allowed any changes in the organization's name or identity.

Statement of Compliance/Non-Compliance:

Therefore, I report compliance with this provision.

Based on the above proof provided, I report overall compliance with the policy.

Report Approval Details

Document Title:	Asset Protection.docx
Attachments:	
Final Approval Date:	Nov 3, 2022

This report and all of its attachments were approved and signed as outlined below:

Stan MacLellan

A handwritten signature in black ink, appearing to be 'SM', with a horizontal line extending to the right.

Todd Rollauer