NORTH THURSTON PUBLIC SCHOOLS

ADMINISTRATIVE CENTER ◆ 305 COLLEGE STREET NE, LACEY, WASHINGTON 98516-5390
TELEPHONE: (360) 412-4400◆FAX: (360) 412-4410

EXECUTIVE LIMITATIONS MONITORING REPORT

EL-4 ASSET AND FACILITIES PROTECTION

FROM: Troy Oliver, Superintendent
DATE: December 10, 2024

The Asset and Facilities Protection Policy focuses on achieving the Board priorities in the district Ends Policies, as well as the Superintendent's aligned Ends Policy Interpretation. This policy ensures the district establishes the necessary policies, procedures, and trainings to protect the District's assets and facilities.

Accordingly, the Superintendent is limited from implementing asset and facilities protection procedures which:

> Policy Criterion 10: Fail to protect district information, including confidential information, files, from loss, damage, theft, and inappropriate use or access. Operate without adequate safeguards to protect the intellectual property of the District.

Superintendent/CEO Interpretation:
The Superintendent will ensure the District has processes in place and takes reasonable measures to protect District information and intellectual property.

Superintendent/CEO Evidence Report:
We have the following safeguards in place for protecting District data:

- **Least Privileged Access** – Staff are only granted access into the systems they require to do their job to mitigate the scope of potential data breaches.
- **Physical Data Security** – Servers and networking infrastructure are in secure rooms. District hard drives are destroyed after the end of their life to protect data.

  Physical File Security – Sensitive files (personnel files, confidential documents) are stored in locking cabinets and/or in secured spaces. Confidential documents are shredded when disposed.
- **End Point** Protection – Robust antivirus software is installed on all District systems as well as strong firewall policies to mitigate external threats to data. Multi-factor authentication protects accounts from unauthorized access. Monitoring technology alerts staff to attempts to circumvent network security measures.
- **Automated Account Access** – Staff accounts are automatically offboarded at point of separation to ensure they no longer have access to privileged District data.

- **Data Security Training** – Staff receive annual training in data security best practices to help mitigate attacks targeting our data. Technology staff engage in training in cyber security.
- **Data Breach Protocols** – In the event of potential data breach, the District has in place a Cyber Incident Response Plan to quickly respond and mitigate potential data breaches.
- **Vulnerability Testing and Review** – The District engages with agencies to test our systems for security vulnerabilities and provide recommendations to continue strengthening data security.
- **Intellectual Property Protection** – NTPS Procedure 2022P – Student Electronic Resources and Digital Citizenship and 5022P – Staff Electronic Resources and Digital Citizenship provide guidance regarding ownership of staff and student work to clarify when work is the District's intellectual property. New staff members review this procedure and are reminded of it through periodic trainings.

Conclusion:

The Superintendent/CEO evidence stated above demonstrates that we are in compliance with Policy Criterion 10 of this Executive Limitations Policy.