Digital Governance Policy P2402

The School Committee recognizes the increasing availability and utility of data for furthering educational goals. For purposes of collecting, managing, and using data, the following policy is provided.

Data Management Plan

The Superintendent or designee shall create and maintain a data governance plan which establishes the vision for the use and management of data in the schools. The Plan shall identify how data is collected, organized, managed, disposed, stored, secured, backed up, and shared, and shall be crafted in a manner that facilitates data analysis and data sharing. The School Committee is aware that the Town of Westford may maintain an Information Security Policy. In cases where any of the topics listed above are addressed by the WPS' implementation of the town policy, the plan may simply refer to the town's information security policy rather than duplicating text, to the extent necessary for ensuring a WPS plan which is complete but avoids redundancy with the town policy. The following guidance is provided for purposes of creating the WPS Data Governance Plan.

Collecting: Data shall be collected as required by law, as required by state regulation, and as necessary to enhance the understanding of how to best serve the students and staff of Westford. To the extent reasonable, planning for the collection of data shall strive to use data which is either already collected or is easily obtained, avoiding the collection of data simply because it is possible to do so.

Organizing: To the extent possible, related data should be stored in a single data collection rather than multiple smaller collections. Additionally, the use of electronic links is preferable to duplicating data in multiple collections; this is to ensure data stays current and is consistently known by all users.

Managing: To the extent practical, and where the law doesn't mandate that data be retained on paper, the WPS shall seek to maintain data electronically. Any vendor or contractor who obtains access to personal and private information of staff or students shall be required by contract to adhere to the same protection policies as employees.

The plan shall define roles and responsibilities regarding maintenance and use of data. It shall also define rules to guide activities associated the creation of sensitive data, the storage of sensitive data, and the required behaviors of staff who acquire data through performance of their job, such as may be the case with teachers obtaining personal student data from colleagues or parents.

Disposing: The plan shall identify when private and personal information is to be disposed of and how it shall be disposed of, consistent with all pertinent laws and regulations.

Training: The plan shall identify what training is to be provided, and the purpose of the training. Possible needs for training include providing staff the understanding of how to use data and where to find specific data within or about the district. Additionally, training must be provided to the custodians of data repositories which store sensitive information about students or staff. Data custodians who manage private data of students or staff shall be trained and assessed at least bi-annually in their adherence to data security practices. The Superintendent shall also ensure role-unique training is provided as necessary to ensure use of data in a manner compliant with this policy.

It is recognized that staff have access to very large amounts of data which may be used to enhance our ability to serve students. The sheer volume of data, however, can be daunting and the School Committee understands that planning for the use of data and the associated training are necessary and valuable aspects of data governance.

Storing: Significant amounts of data are required for the efficient operation of the school district. In order to retain cognizance of the various data available in the district, the WPS shall maintain an inventory of data collections, their locations, and their respective custodians. This inventory catalog shall indicate the types of data retained in each collection, and the catalog shall be accessible to staff online.

Securing: Much of the data maintained in the WPS is confidential. This includes both student educational and health information and staff personnel information. Data shall be secured as required by law, such as FERPA, and by this policy as detailed below.

Backing Up: The plan shall establish a strategy for backing up information, identifying the repositories to be backed up, the frequency, and the person responsible.

Sharing: To the extent practical, aggregated, de-personalized information should be made available in a manner which is distinct from that used to access more private information. When creating new digital data collections or updating the software used for existing ones, the WPS shall seek products that are compatible for purposes of exchanging data.

Auditing: Regular audits of retained data shall be conducted in order to ensure the currency and validity of the data, and compliance to the pertinent laws and regulations, as well as to the Data Governance Plan. Audits should also be used to identify opportunities for consolidation or linking of repositories, where it is sensible to do so for purposes of efficient district operations. Audits may be conducted by any designated staff who have been trained to conduct these audits and who are not primary contributors to nor custodians of the repository (ies) in question.

Use of Data

The School Committee and Superintendent shall seek to use data to guide decision making. When new programs or initiatives are to be introduced, planning shall be conducted which identifies the data to be used for evaluating the effectiveness of the new program or initiative. Where data is used, the analyst will strive to ensure the data is current, relevant, and of high quality.

When seeking approval from the School Committee for a major change to the staffing structure, curriculum, or policy implementation at any WPS school(s) the administration shall articulate measures which may be used to assess the effectiveness of the proposed change in meeting the intended goal(s) of implementing the change. While not all goals lend themselves to measurement, candidate measures shall be provided where measurement is feasible and practical.

It is expected that over the course of the school year district staff will evaluate the data which planning has identified to be insightful indicators of district performance. Also, in accordance with P2102, the Superintendent will use data at the end of each school year to evaluate district performance, and will present this analysis in his or her presentation of suggested goals to the School Committee each fall. Where any of these ongoing analyses or year-end analyses suggest that it would be desirable for the district to take action, the data and analysis shall be provided to the School Committee as rationale for the suggested action and/or funding request.

Data Security

The Superintendent or designee shall establish security measures which ensure both confidentiality of private data and the security of the data repositories in which they reside. As a minimum, the use of complex passwords is to be required for any equipment, including mobile devices, with access to sensitive information. The Superintendent shall establish mechanisms which assess ongoing compliance to all security measures put in place. The WPS is expected to adhere to the Town of Westford's Information Security Policy, but the

Superintendent shall notify the School Committee if any costly actions are required in order to maintain compliant to the town's policy, or if any facet of the town's information security policy is contrary to this policy.

The Superintendent or designee shall identify what information must be kept secure and where it resides. The WPS shall employ a need-to-know test for access to any sensitive information. Access should be provided as needed to further educational goals, but effort should be made to minimize the amount of personal data provided, without compromising the goal in question. This should not be construed as a restriction on the ability of staff to obtain access to any information which allows them to better perform their jobs or better service student(s). Additionally, the caregiver of any student and any staff member shall be provided access upon request to any of their respective personal data being retained by the WPS.

In any instance where private information may have been inadvertently made available to the public or to unauthorized individuals not affiliated with the WPS, the caregivers of any affected student or the affected staff member(s) shall be notified immediately. If it is determined that private information was compromised, the Superintendent shall ensure that the incident is investigated such that measures can be taken to reduce the risk of any further such incidents. In cases where the disclosure rises to the level of a legal breach, the WPS shall adhere to the requirements of MGL CH 93H.

REFERENCES

Federal Educational Rights and Policy Act (FERPA)

Massachusetts General Law (MGL) Chapter 93H: Security Breaches

Town of Westford Information Security Policy

P6111 – Student Records

Policy Adopted: June 20, 2016
Policy Reviewed:
Policy Revised

WESTFORD PUBLIC SCHOOLS
Westford, Massachusetts 01886