Advisory Note 1

Protocol for Receiving and Transmitting Protected Information

DEFINITION OF PROTECTED INFORMATION

Protected information is information in any form including a combination of an individual's name and an account number, or other personally identifiable information. This information includes, but is not limited to, the following: documents containing social security numbers, credit card numbers, dates of birth, financial account numbers, drivers' licenses or ID numbers, and medical receipts/records.

If you are unsure if a document or information is protected, contact IT support or adhere to the below protocol to ensure the security of this information.

ACCEPTABLE METHODS: TRANSMISSION AND RECEIPT OF PROTECTED INFORMATION

Transmission

The following are acceptable methods by which protected information may be transmitted:

1. Mail
2. Fax
3. Secure Internet (e.g. https://message.coursevector.com; secure online payment portal for purchasing)
4. Phone

Receipt

The following are acceptable methods by which protected information may be received:

1. Mail
2. Coordinated Fax (documents containing sensitive information should not be left unattended)
3. Secure Internet (e.g. - https://message.coursevector.com; pay.boroughs.org)
4. Phone

PROHIBITION FROM SENDING OR RECEIVING PROTECTED INFORMATION OVER E-MAIL

Sensitive information may not be transmitted or received through e-mail. If staff is in receipt of such information over e-mail, unsolicited or otherwise, the following procedure applies:

1. Staff member should notify IT support with the subject, date, time of the e-mail.
2. IT support will delete the e-mail from the server.
3. Staff member will delete the e-mail from their inbox by holding shift and pressing delete (permanent delete).
4. Staff member will then notify the sender, in an email, that they should not send protected information via e-mail and inform them of alternatives for sending the information.

Advisory Note 1 (continued)

SAMPLE E-MAIL REPLY

The following sample reply may be used when replying to an individual that has sent you protected information over e-mail:

> For security purposes, please do not e-mail any sensitive personal information (e.g. social security numbers) or documents which contain such items. If you wish to provide PSAB with any of that information you may use the following fax number: _____.
>
> You may also send the information through our secure message portal, https://message.coursevector.com.

Advisory Note 2

Guest Access and Secure Areas:
Procedures for Personal and Information Security

GUEST BUILDING ACCESS

PSAB's offices do not require automatic or guaranteed access to guests. Accordingly, for security purposes, all guests should be screened before entering the building. The verbal screening should identify the guest and if they are expected at PSAB offices. If unexpected, the screening should ensure they have a legitimate reason to be visiting PSAB.

If, during the screening process, it is clear a prospective entrant is not visiting for official business, or is a perceived threat, they should be declined entrance. If, in the discretion of staff, a guest is an apparent threat to the safety of PSAB employees or property, staff should contact police for assistance. Guests granted building access should be accompanied by PSAB staff when in the building.

SECURE AREAS

Secure areas are offices or other areas of the building where sensitive or protected information is kept requiring a key fob for access. These areas should be locked when unoccupied. Only staff requiring access to information stored in these secure areas to perform their job should occupy these areas alone. Other staff may access these areas if accompanied by a staff member that requires access to perform their essential job functions. Likewise, guests should not be permitted to access secure areas unless accompanied by a staff member that requires access to secure areas to perform the essential duties of their job.

Advisory Note 3

Email Security Procedures

RECEIVING SUSPICIOUS EMAILS

Staff in receipt of the suspicious email, including suspect emails soliciting a reply with protected information, should immediately forward the email in question to PSAB IT support (IT@boroughs.org). Staff in receipt of such an email should not forward the email to other staff or anyone else.

If a member of PSAB staff believes they may have replied to, opened an attachment, or weblink in a suspicious email, the staff member should notify PSAB IT support immediately by forwarding them the email and providing details on what occurred.

In the event a staff member believes their computer may have been infected after taking action on an email, said staff member should shutdown their computer or disconnect their computer from the network until IT support is available to assist.

If it appears a legitimate email was quarantined by malware protection software and is identified as potentially malicious, staff should forward the quarantine summary email to IT support to review. If the email is verified by IT as legitimate and safe, it will be released from quarantine.

RESPONDING TO MEMBERS

If staff is in receipt of communications—email or otherwise—from members or other PSAB stakeholders, indicating that they received a suspicious email from PSAB, the following procedures apply:

- If it is clear that the email was not generated by PSAB, after notifying PSAB IT support, you may respond letting the member know that the email did not originate from PSAB and that they should refer the email to their IT consultant.

- If it is not clear whether the email in question was sent from PSAB, coordinate with PSAB IT support before responding to the member/PSAB stakeholder.

PROHIBITION FROM SENDING PROTECTED INFORMATION VIA EMAIL

Protected Information, as defined in Advisory Note 1, should never be emailed to a requester. Such sensitive information should only be sent via an acceptable means outlined in Advisory Note 1.

Advisory Note 4

Storage of Records Containing Protected Information

PHYSICAL RECORDS

Physical records that include protected information must be kept in secure office areas. Records containing protected information should not be stored outside of these secure areas.

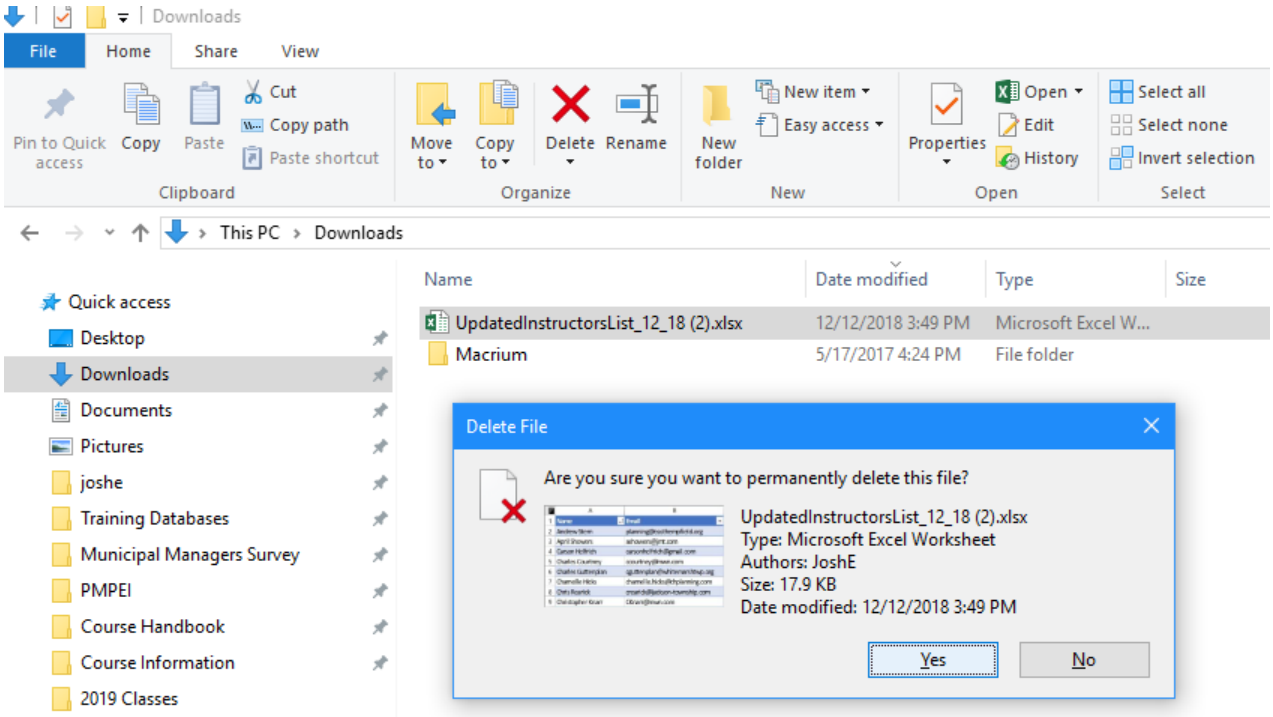
Records including protected information that do not need to be retained or stored should be destroyed—disposed of in a way that the record cannot be reproduced, (i.e. shredded for paper records)—as soon as they are no longer needed for a business purpose.

To review what constitutes protected information and secure office areas, see Advisory Notes 1 and 2 respectively or consult with IT support.

ELECTRONIC RECORDS

Only computers in secured areas that utilize file encryption set up by IT support may store protected information electronically.

Electronic records containing protected information that are downloaded from a secure internet service on a computer outside of a secure area should not be saved on the computer. If the file is downloaded for printing, the file should be deleted from the computer's temporary downloads folder using shift-delete to permanently delete the file after printing (see screenshot below).



If you have questions on how to delete a file containing protected information from your computer, contact IT support.

Advisory Note 5

Password Management

PASSWORD MANAGEMENT PROCEDURES

Unless otherwise noted by IT support, passwords for all work-related accounts and applications are to be filed with IT support for emergency recovery purposes. When a work-related password is updated, IT support should be notified of the change and the new password in a secure manner: hand delivered, via a secure message service (e.g. - secure.coursevector.com), or through another secure application designated by IT support. Password changes should be communicated to IT support as soon as possible following a password update/change.

Strong passwords should be used for applications that involve protected information. A password is general considered strong if it has eight or more characters including a minimum of one capital letter and one special character. Software applications and internet accounts that involve or store protected information should never have associated account passwords that are weak or too generic (e.g. - PSAB123, password, boroughs2019, etc.). If you have questions on whether a password is strong enough for a given application, contact IT support.

Passwords should be stored using the encrypted excel files prepared by IT support on staff computers or through another secure application designated by IT support for password storage. Passwords should not be stored haphazardly in easily accessible, unsecured locations (i.e. – notes posted on a desk).

Passwords should not be shared among staff unless expressly approved by management.

Advisory Note 6

Remote Work and Information Security

Remote work, as authorized by PSAB management, is only permitted in accordance with the following provisions to ensure information security:

a. Company issued equipment
Remote work that involves PSAB network access may only be conducted on a device issued by PSAB. PSAB staff should not adjust any settings or download any software on their issued device without the express consent from their supervisor or PSAB IT support.

b. Protected information access and storage
No protected information, as defined in Advisory Note 1, should be stored directly on the staff issued device. Protected information should only be accessed through the secured remote connection as authorized.

c. Remote printing and storage of protected information excluded
PSAB staff should not print any protected information at, or to, an offsite location or store protected information offsite unless expressly approved by their supervisor. PSAB IT support will disable offsite printing features on staff devices with access to protected information.

d. IT support consultation
Staff with questions on security and remote work should contact PSAB IT support. PSAB IT support will conduct routine reviews for compliance with this advisory note and to answer questions regarding remote work and information security.

e. Suitable remote work environment
PSAB staff working remotely must maintain a workspace that is safe and conducive for the performance of their duties. At a minimum, staff working remotely must have access to high-speed internet; be able to send, receive and respond to electronic mail; and communicate via telephone. The workspace should be free from hazards and kept in good order. Remote work should not be conducted in public spaces where protected information or other PSAB related work would be viewable by others that otherwise would not have access to the information.