PRINTING SENSITIVE INFORMATION? - READ THIS!

NWT OIPC Guidance on Printing Sensitive Information, May 2020

Cause for Issuing Guidance:
In response to recurring incidents of privacy breaches in both government and health settings across the NWT caused by documents being directed to the wrong printing station, the OIPC offers the following guidance.

This guidance applies to all public bodies, agencies, contractors and volunteers when printing sensitive information. Sensitive information may include but is not limited to *personal information, personal health information*, *privileged information*, etc.

Issue: Documents being printed on the wrong printer, largely as a result of employees relying on the assumption that a workstation is connected to a particular printer or because the wrong printer has been selected.

Risk: Unauthorised disclosure contrary to GNWT/Ministerial policy and legislation.

Compliance Requirement and Legislative Reference: Key Sections of the *Health Information Act* and *Access to Information and Protection of Privacy Act* include but are not limited to section 2 of ATIPPA, section 8(a) and (c) of the HIA and sections 13 and14 of the HIA Regulations.

Background:
GNWT Departments and agencies interconnect electronically through a common network in order to permit the use of shared resources, such as backing up data, advantaging network security, and shared use of equipment and services, such as multifunctional printers/fax/copiers.

Public bodies may use a combination of shared printers (available to many computer workstations) as well as “personal” local printers (often connected to a

single workstation). Shared printers are used my many people, while personal computers are most often assigned to one employee. Further, a workstation may be used by one or more employees on a regular basis, or be used temporarily and/or irregularly by causal workers.

There have been a number of incidents in which, in using a workstation to print documents, an employee has printed to the wrong printer. When this occurs sensitive information may be disclosed to not only the wrong person, but because printers are often a shared service connected over a shared network, documents might be printed to the wrong business unit, and even the wrong department or agency. There has been at least one incident in which a document was sent to a printer in a different building some blocks away.

This situation may result in unauthorized disclosures of sensitive information to the 'wrong' person or more specifically, to a person who has no need to know that information. Such events can cause a reasonable probability of harm to one or more individuals or the organization the information is about. When these incidents occur, and recur, the public and business stakeholders may lose faith in a public body's ability to protect sensitive information. Stakeholders and the public may be less willing to share sensitive information with government in future, which weakens capacity of the government to provide public services.

Guidance - Privacy Best Practices when Printing:
We recommend the application of administrative, physical and technical safeguards to protect privacy and prevent errors from occurring when printing documents.

Here are four approaches you can use to protect privacy when printing:

1. **Preconfigure Printer Settings – limit print options;**
2. **Apply Pre-print Checklist – verify your printer before hitting "print";**
3. **Use Secure Print Setting – control document by printing in "real time";**
4. **Use a Cover Page – prevent inadvertent access by others.**

1. **Configure Printer Options – limit print options**

   Ask your IT / technical support staff to pre-program your workstations to limit printing options, so staff can only print to one, or to a limited number of printers, from that workstation. The wrong printer can't be printed to it if it cannot be selected from the electronic list of printer options.

   Where this is not possible, managers should verify the correct printer has been selected as the default printer on work stations and be sure to communicate with staff, and use clear policies and procedures, to ensure that altering printer settings is not permitted without prior authorization.

2. **Apply Pre-print Checklist – verify printer before hitting "print"**

   This "checklist" is simple: Step 1 - Verify. Step 2 - Verify. Step 3 - Verify.

   To use this approach, create a word document containing the word "test" and your name. This is your "test" document. Send the document to the printer you intend to use. Physically check the printer to verify if your test document has indeed printed out on the printer as you expected.

   If "yes", you can print sensitive information on that printer using that workstation so long as you are reasonably certain that the print setting cannot or has not been changed since you last printed.

   If "no", understand where the document was printed. Physically verify the name of the printer you want to print on (you may also verify this with your IT help desk staff). Then, in the computer printer settings, verify that the name of the printer appears in the printer settings, and select the printer as your new "*default*" printer.

   If you still cannot print to the desired printer, ask for help from your supervisor, or your IT support desk. You might also select another printer and start over, printing a test page to that printer, etc..

It is particularly important that this approach be used by new or returning employees. It is also important to re-verify the printer that a workstation is sending documents to after any physical installation of a new or re-install of an existing computer, and/or after any network or local end point re-configuration, or physical installation of a new or existing computer or printer. The setting should also be verified if a temporary worker has been using the workstation, as they may have changed the settings.

3. **Use Secure Print Setting – control document by printing in "real time"**
   Many newer model printers, especially multifunction printers have a printing option called "secure print". Secure print, or similar function, allows pre-setup of printing options to prevent printing without use of a user selected code. When using secure print, documents sent to the printer do not print, and instead the documents queue electronically until such as time as the user physically goes to the printer, enters their user code on the keypad, and selects print.

   This allows all or selected documents sent to the printer to be physically printed by the user while they are at the printer observing the documents printing, and preventing others from having access to the documents. Use of this approach is beneficial as it prevents sensitive documents from being left unprotected on a printer. Also, if the wrong printer is selected by the user, the documents will not print out, so no one will be able to inadvertently view the contents of the documents.

   This is a great approach to use when several employees use the same printer. This obviously has the added benefit of efficiencies, of not having to sort through piles of documents that are not the user's to find their own printed documents. It does require the user to stand by the printer while documents print out after the user enters their user code and this may be a little more time consuming.

A caveat of this approach is that no personal identifiable information should be included in the document title. Using, for example, a person's name in the title, will result in this displaying in the print queue list, viewable in the electronic display window on the printer.

4. **User ID Cover Page – prevent inadvertent access by others**
   As an added measure of prevention, users can set up their work stations to print a cover sheet with each document they print. This cover sheet clearly identifies the document as unique from other printed documents and prevents others from seeing what was printed in the main document, when they pick up printed documents from the printer.

   The downside to this is it uses considerably more paper (and ink), so using the first three approaches may be better. The most effective approach is the secure print option (only printing documents when physically at the printing station) if the type of printer has this feature this and it if feasible.

Understanding Roles and Responsibilities:

Applying this guidance requires that technical and operational staff, as well as management take on certain roles and responsibilities to ensure this guidance is applied where feasible.

Staff should follow this guidance and make inquires if they are not sure about printer settings, or have printer issues before committing sensitive information to being printed. Management should ensure all endpoints have been appropriately configured to print on the correct printer, take steps to limit print options where feasible, and ensure staff are aware of how to protect privacy when printing.

IT and technical service desk staff should take steps to ensure they inquire with local managers to identify the correct printers for the business area. IT and technical staff should not make assumptions about which printers should be set as the default. As an alternative, IT and technical staff might be requested to not configure print services at all. In which case the operational manager should be

made to ensure their employees configure their own workstations to select a particular printer as directed. This approach prevents printing until the defaults have been set by the user, but does come with the risk of staff unfamiliar with configuring printers making mistakes and defaulting to the wrong printer. Preferably, managers should be aware of which printers are available and which their staff should be printing to, and direct IT/ technical staff to pre-configure a limited number of print options for each workstation under their control.

Note: Anyone that receives printing in error should take immediate steps to secure the document and contact the sender, to determine next steps.