

<b>Administration</b>	<b>Corporate</b>	<b>Board Approved Date:</b>	<b>21-02-24</b>
<b>Policy</b>	<b>Privacy and Confidentiality</b>	<b>Revision Date:</b>	<b>N/A</b>
<b>Policy No.</b>	<b>20-079</b>	<b>Internally Approved Date:</b>	<b>21-02-12</b>
References	Housing Services Act, 2011 Personal Information Protection and Electronic Documents Act, 2000 Occupational Health and Safety Act, 1990 Workplace Violence and Harassment Policy (Human Resources Handbook) Records Management Policy Dispute Resolution Policy		
Forms	Checklist for PIPEDA and HSA Sample Confidentiality Agreement		

### 1. Policy Statement

In accordance with its obligations under the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, the *Housing Services Act (HSA) Regulation 367/11*, and the *Occupational Health and Safety Act (OHSA)*, DRNPHC will protect the privacy and confidentiality of the applicants, tenants, employees, board members, volunteers, and other stakeholders by ensuring the appropriate treatment of their personal information.

### 2. Purpose

The purpose of this policy is to ensure DRNPHC's compliance with the PIPEDA, the HSA and O. Reg. 367/11. Together, these pieces of legislation set out standards for the collection, use, disclosure, and protection of personal information gathered through the administration and operation of non-profit housing.

This policy also sets out the conditions under which personal information may be shared with staff or volunteers in order to protect them from experiencing workplace violence, harassment, or domestic violence in the workplace in accordance with the *Occupational Health and Safety Act*.

### 3. Scope

This policy applies to the personal information collected by DRNPHC from applicants, rent-geared-to-income and market rent tenants, staff, board members, volunteers, and others.

### 4. Definitions

Personal information

Refers but not limited to the following types of information:

- an individual's personal address, telephone number, or email address
- any identifying number assigned to an individual which can lead to their identification (e.g. Social Insurance Number)
- information regarding an individual's income and assets
- bank account and credit card information
- information about rent payment history
- information relating to the race, national or ethnic origin, citizenship status,

colour, religion, age, sex, sexual orientation, marital or family status of an individual

- information relating to the education, medical, psychiatric, psychological, criminal or employment history of the individual
- credit and rental history reports
- financial information for the purposes of establishing rent-geared-to-income assistance
- an individual's blood type or fingerprints
- information about an individual's personal or political opinions
- correspondence sent to DRNPHC that is of a private or confidential nature, and any replies from DRNPHC that would reveal contents of the original correspondence
- the individual's name if it appears with other confidential information (e.g. rental arrears reports)
- employee information including résumés, salary and benefits, disciplinary action, bank account information, tenant complaints about the individual, and problems between staff

#### Personal safety plan

A course of action developed between a staff member and the DRNPHC to help prevent that staff member from domestic violence.

#### Privacy officer

Refers to the individual responsible for the organization's compliance with all privacy legislation.

#### DRNPHC

Refers to the organization whose board of directors has approved this policy.

#### Unauthorized individual

Refers to an individual who is not authorized to view the personal information in question.

#### Workplace violence

Means the same as the definition in DRNPHC's Workplace Violence and Harassment Policy, as stated in the Personnel Manual, Section B Health & Safety, Workplace Violence page 35 and Workplace Harassment and Anti-Discrimination page 30

#### Workplace harassment

Means the same as the definition in DRNPHC's Workplace Violence and Harassment Policy, as stated in the Personnel Manual, Section B Health & Safety, Workplace Violence page 35 and Workplace Harassment and Anti-Discrimination page 30

## 5. Procedure

### a) The Privacy Officer

DRNPHC will appoint a member of staff to act as the privacy officer for the organization. DRNPHC's Privacy Officer is the Director, Tenant & Housing Services, available at (905) 436-6610 and [drnphc@durham-housing.com](mailto:drnphc@durham-housing.com).

The responsibilities of the privacy officer are:

- to review DRNPHC's policies and practices with regard to personal information
- to implement the necessary changes to guarantee that the collection and retrieval of personal information follow DRNPHC's policy
- to inform the tenants and public on how DRNPHC treats personal information
- to respond to complaints, questions, and requests for personal information made under this policy

DRNPHC will, on all forms which pertain to the collection of personal information, identify the name and title of the privacy officer, along with contact information.

b) Collection of information

Personal information will be collected mainly for the following purposes:

- to assess tenancy and determine appropriate unit type and size
- to determine income and assets for rent calculation
- to demonstrate compliance with funding requirements
- to protect the health and safety of the tenant
- to ascertain service levels required in special needs housing
- to conduct reference and employment checks
- to retain relevant information on employees for government reporting purposes
- to assist a member of staff to design and implement a Personal Safety Plan for the workplace

Staff will not seek out personal information about tenants or applicants unless it is relevant to their work. All documents used for collection of personal information will include:

- the purpose(s) of the collection
- the reasons for collection, including the fact that the information may be shared as necessary for the purpose of making decisions or verifying eligibility for assistance under the *Housing Services Act, 2011*, the *Ontario Disability Support Program Act, 1997*, the *Ontario Works Act, 1997* or the *Day Nurseries Act*, or as authorized by an agreement under section 171 or 172 of the *Housing Services Act, 2011*
- the name, title and contact information of the privacy officer who can answer questions and respond to complaints about the collection, use or disclosure of the information
- a consent form to be signed by the applicant or tenant authorizing the collection, use, verification and disclosure of the information being collected

c) The protection of information

All staff, board members, volunteers, and any other individuals who may have access to applicant, tenant or employee files will be required to sign a confidentiality agreement.

Applicant, tenant and employee files must be safeguarded against unauthorized access.

- Paper copies of applicant/tenant information and employee information must be stored in a locked filing cabinet. Secure storage facilities must be provided for archived applicant/tenant/employee and accounting information.
- Databases containing files with personal information, and other confidential electronic files must be password protected against unauthorized access.

- Screen-savers and/or other security measures will be used to protect confidentiality of personal information on computer monitors.

Access to records containing personal information will be granted only if access is required in order to fulfil the designated individual's duties.

When communicating tenant issues to the board, staff will use non-identifying information as much as possible. For example, arrears reports will use codes in place of the actual names of tenants, or summary information will be provided.

All staff have a responsibility to ensure that unauthorized individuals do not have unsupervised access to areas where files are kept and used.

Personal information will be disposed of at the end of the required storage period for tenant records; seven years after the tenant has moved out, and seven years after the end of the fiscal year for financial records.

Paper-based personal information must be shredded prior to disposal. Electronic media must be purged prior to disposal.

d) Release of information

No personal information will be released to third parties without the written consent of the individual (for example: credit references, tenant or personal references). When responding to inquiries for references, staff must limit information provided to the questioner and confirm only the information already provided by the individual making the inquiry.

It is not necessary to have a signed consent to release information to collect a debt, for example to a collection agency, or for a Landlord Tenant Board or Small Claims Court action.

Staff will confirm the identity of the people to whom information is released.

Personal information can be released to the following:

- Funders and auditor: DRNPHC in order to be in compliance with funding program requirements, must release information to funders and auditors. People doing these jobs have their own professional code of ethics and are required to maintain confidentiality. Staff will confirm that the person concerned is seeking access legitimately.
- Access Centre: As part of its responsibilities to the coordinated access system, DRNPHC will provide the access system with information about tenants who have left in arrears. This information will be used by the coordinated access system as part of their screening process for applicants for non-profit housing.
- Researchers: Occasionally, DRNPHC may be asked to assist an approved accredited researcher. Authorization to have access to files will depend on their credentials and the nature of their research. The Chief Executive Officer (or designate) must approve all such requests for personal information.

- Credit bureaus: Information on orders or judgements for money owing will be provided to any credit bureau of which DRNPHC is a member.
- Law enforcement: While DRNPHC has a responsibility to protect the right to privacy of applicants and tenants, this responsibility must be balanced with an obligation to protect the broader community. Law enforcement agencies requesting personal information about applicants, tenants, employees, board members or volunteers, for example confirmation that they live or work at DRNPHC, will be required to provide a written request or “warrant” before information will be released.
- Health and safety officials: Personal information will be provided to outside agencies, individuals and institutions when it can be clearly identified as contributing to the applicant or tenant’s benefit, for example, information about an individual’s medical condition to the paramedics or fire department.
- Next of kin or emergency contacts: It may be appropriate to use personal information to contact a community service agency or a designated relative in exceptional circumstances, such as, when using an emergency contact provided by a tenant and held on file, or contacting medical support services when a tenant is unable to function and maintain his/her tenancy.
- In the case of suspected child abuse, information will be provided to the Children’s Aid Society. (This duty to report is required under Section 72 of the Child and Family Services Act.)

Personal information may be released to the police:

- In the context of reporting criminal activity, staff with personal knowledge will report the incident.
- With respect to crimes against persons, witnesses are obligated to report and provide appropriate information to the police so that charges can be laid.
- If there is a substantiated reason to suspect criminal activity, such as drugs or gangs, staff with knowledge of the activity will report it to the police.
- Victims of crimes are responsible for reporting the crime directly to the police. However, if the victim is a child or a person with a disability that renders them incapable of making the decision to report, and an individual has knowledge of this crime, the legal responsibility lies with all citizens and DRNPHC to report the crime to the police.

e) Access to and correction of personal information

The privacy officer will respond to all requests for access to or correction of personal information.

An individual who provides satisfactory identification will be informed of the existence, use and disclosure of his or her personal information and will be given access to that information. The privacy of others’ personal information must be protected when giving an individual access to their own personal information.

However, if the privacy officer believes that releasing personal information to an individual would prejudice the mental or physical health or security of any person, he or she will not release the information.

Information contained in the file will be reviewed prior to providing access to the file and may be redacted or edited as necessary to protect the privacy and personal information of others.

An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate. If the privacy officer is not in agreement with the individual's request for correction, a written counter-statement explaining why the information should not be amended will be provided to the individual and filed with the original information.

f) Procedure for handling complaints

The privacy officer will respond to all complaints about collection, use, disclosure, storage and disposal of personal information within thirty (30) days of the request being made, and advise the complainant as to the action that has been taken.

Each complaint will be assessed to determine whether:

- the collection of personal information is necessary
- the information was collected, used, released or disposed of inappropriately
- DRNPHC's policies and procedures need to be modified
- disciplinary or other action needs to be taken with respect to a breach of a confidentiality agreement

Where necessary, the privacy officer will make the necessary recommendations to the Chief Executive Officer in connection with resolution of the complaint.

g) Prevention of workplace violence

DRNPHC, as part of its Workplace Violence and Workplace Harassment policies, must notify staff, contractors, casual workers, and volunteers if there is the risk of workplace violence from any person (including tenants and co-workers) with a history of violent behavior if:

- they can be expected to encounter that person in the course of their work
- the risk of workplace violence or harassment is likely to expose them to physical injury

Tenant and employee personal information, disclosed in accordance with DRNPHC's Workplace Violence and Workplace Harassment policies, is permissible and will not be considered a breach of confidentiality.

h) Breach of confidentiality

The following constitute breaches of confidentiality:

- Discussion of any confidential information within or outside the organization where it may be heard by individuals who are not authorized to have access to that information.
- The provision of confidential information or records to unauthorized individuals.

## ADMINISTRATIVE POLICIES - CORPORATE

- Failing to secure written or electronic personal information which results in the information being visible, or potentially visible, or distributed to unauthorized individuals.
- Deliberately accessing confidential material that is not required by that individual in the performance of their duties.

A breach of confidentiality may be grounds for staff to be disciplined or terminated.

A breach of his or her confidentiality agreement may be grounds for a board member to be removed as a director of the corporation

All others associated with DRNPHC who sign a confidentiality agreement (volunteers, contractors, etc.) will be held to the same standard as staff and board members.

End.